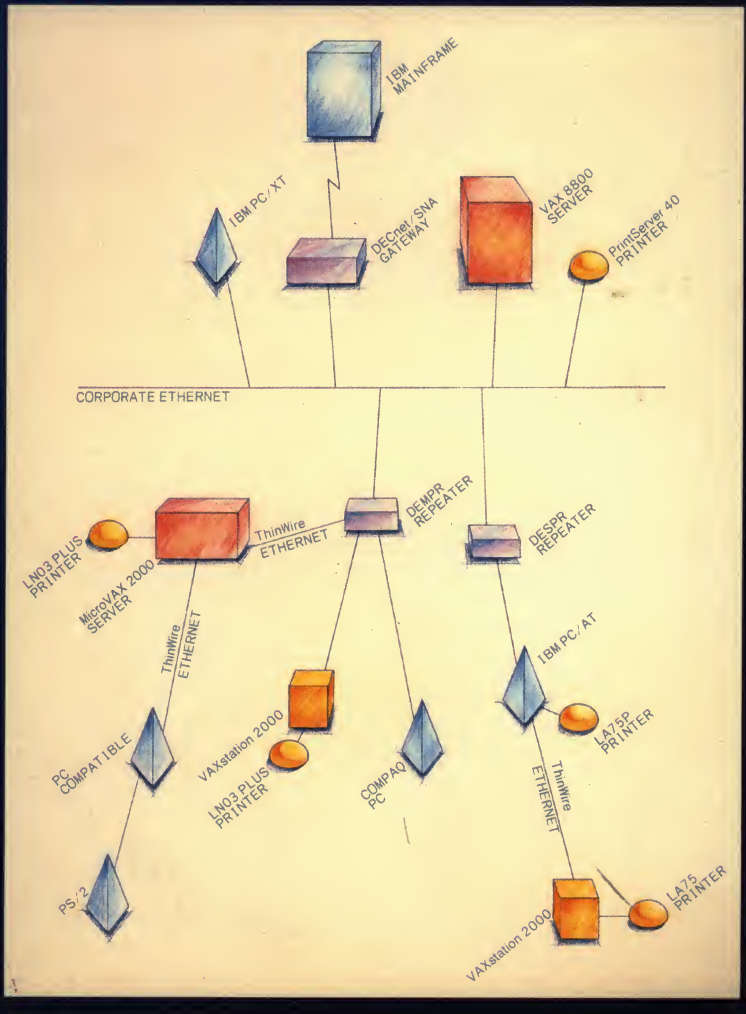
Integrated Personal Computing Handbook

digital



Integrated Personal Computing Handbook

digital

Table of Contents

Chapter 8 • The User Environment

Chapter 9 • DECnet-DOS

Chapter 10 ▪ International Character Sets and Keyboard Support

Chapter 11 ▪ Integrated Personal Computing Resources

Glossary

Index

Figures

Tables

Preface

Digital's integrated personal computing products are an extension of Digital's systems and networking architecture and merge the VAX/VMS and MS-DOS environments. Using the Personal Computing Systems Architecture (PCSA), Digital's personal computing network consists of VAX or MicroVAX servers, running VAX/VMS Services for MS-DOS and DECnet/PCSA Client software that runs on IBM personal computers (PCs) and IBM compatibles.

PCSA provides a framework for integrating personal computing into an organization's total information system so that different types of users can share information, large system resources, and network services across the entire organization. This architecture provides better computing and communication capabilities than those of conventional PC LANs (personal computer local area networks).

The purpose of this handbook is twofold: to familiarize the reader with Digital's integrated personal computing solution and to explain how it can increase the power of PCs.

This handbook is intended for readers who understand communications technology and who want to learn more about Digital's integrated personal computing products. System administrators and designers who are considering using PCSA to expand the capabilities of their existing systems will also find this handbook useful. The handbook includes the following components:

The *Executive Summary* gives a brief overview of the contents of the handbook and Digital's personal computing integration strategy.

Chapter 1 describes the services that servers provide to PC clients on a network.

Chapter 2 provides technical information about the integrated personal computing hardware configurations.

Chapter 3 informs the system administrator about setting up and managing PCs in a network.

Chapter 4 gives results from Digital-sponsored tests on three network configurations. This chapter also suggests methods on how to plan and fine tune the network for better performance.

Chapter 5 discusses how to secure PC data in a network.

Chapter 6 discusses how to install third-party software on the server.

Chapter 7 describes the network layering and session interfaces. This chapter also explains the DECnet-DOS programming concepts.

Chapter 8 discusses some of the tools available to the user and explains how to use the PC network environment.

Chapter 9 provides an overview of DECnet-DOS networking software.

Chapter 10 lists the Digital-supported character sets and keyboards.

Chapter 11 gives a list of available resources including educational and technical services.

The Glossary defines terms used throughout this handbook.

Executive Summary

Digital Equipment Corporation is the leading producer of networking products and services that deliver computing power directly to an individual's workspace. Digital's computing philosophy is based on the concept of distributed processing, which means bringing powerful applications where they are needed: offices, laboratories, factory floors, or any workspace that can benefit from shared information or computing resources. Digital distributes networked computing power through a broad range of products and services.

Digital's integrated personal computing products broaden the company's networking environment by extending the power of DECnet/OSI and VAX/VMS to leading MS-DOS computers. Thus customers can choose from Digital, IBM, COMPAQ, Olivetti, Zenith, Apple (in the near future), and other vendors of desktop devices.

Using Digital's open networking environment, each user can take advantage of the organization's total computing capabilities by exchanging information and sharing resources. Small systems can access the greater computing power of larger systems or run applications best handled by PC workstations.

Digital's Personal Computing Systems Architecture (PCSA) provides the best available solution for integrating PCs in a corporate computing network. Using PCSA, PC workstations can connect to Digital's VAX/VMS computers and share data and files with other users on the corporate network. PCSA provides:

- Direct, system-wide access to shared applications and data files
- Direct, system-wide access to physical resources, such as disks, printers, and network gateways
- Centralized management of end-user computing, including the ability to boot workstations over the network while retaining all the benefits of standalone personal computing
- Integrated MS-DOS and VAX/VMS environments
- Expansive multivendor compatibility based on DECnet/OSI, MS-NET, MS-DOS, and NETBIOS

▪ Servers and Clients

PCSA servers and clients can be networked into countless configurations. Digital's PCSA product set was designed to deliver the full set of network services to the many types of PCs that exist in organizations today.

In the PCSA environment, any VAX machine—anywhere on a local or wide area DECnet network—acts as a server to selected PC clients. The server software, called VAX/VMS Services for MS-DOS, is a layered application that allows VAX and MicroVAX computers to act as application, file, disk, and print servers for PCs in a DECnet network. It lets PC users access remote printers and disk files as though these resources were local.

DECnet/PCSA Client software allows selected PCs to be connected to VAX or MicroVAX computers in a DECnet network. DECnet/PCSA Client software is a superset of DECnet-DOS—that is, all of the programming tools included in DECnet-DOS are included with the DECnet/PCSA Client software. DECnet-DOS also is available as a separate PC connectivity product for PC users who require *only* or *primarily* task-to-task programming tools for customized applications or access to ULTRIX or RSX operating systems.

Both Digital and selected non-Digital PC workstations work equally well in network configurations ranging from standalone PC LANs for a small organization to fully configured DECconnect networks that integrate data, voice, and video communications into a comprehensive, enterprise-wide network.

▪ Network Management

Networks of all sizes require some degree of network management. PCSA provides the following guidelines for setting up and managing a network environment:

- Assigning user privileges and system access
- Assigning print queues
- Allocating disk space
- Maintaining and upgrading server-based PC applications
- Devising custom-integrated solutions
- Performing disk backups

▪ Performance

Managing the network also includes monitoring network performance. When a PC network is integrated into a VAX/VMS environment, its optimum performance is critical. In comparative tests between PCSA configurations and competitive offerings, the PCSA configurations performed exceptionally.

In a predefined "typical office scenario," Version 2.0 of VAX/VMS Services for MS-DOS running on a MicroVAX II supports 30 simultaneous users with performance comparable to or better than a standalone IBM Personal Computer AT with a hard disk.

In general, the performance of VAX/VMS Services for MS-DOS depends on a number of factors:

- Size of CPU
- Configuration of disks
- Network usage characteristics, including the ratio of active to nonactive users, peak loading trends, and workload

Digital's testing procedures and certification standards are among the most comprehensive in the industry to ensure compatibility and connectivity to the Ethernet LAN environment. Ethernet is a high-speed data communications protocol.

▪ Network Security

PCSA provides security procedures for PCSA file servers and virtual disk services, ensuring that information is protected from unauthorized access. However, security measures do not impact the ability of authorized users to work comfortably with the network. With PCSA, authorized users can use services such as the application interface to load third-party software and to create custom programs that run on the network.

▪ Programming Interface

Version 2.x of VAX/VMS Services for MS-DOS supports the NETBIOS programming interface to create custom programs. NETBIOS applications run unmodified on client PCs. NETBIOS applications can then communicate transparently over both LANs and wide area networks (WANs). NETBIOS applications also can talk to non-PC DECnet nodes such as VAX/VMS and ULTRIX.

• User Interface

The user's environment reflects PCSA's flexibility and usability. PCSA currently uses the Microsoft Windows (MS-Windows) interface. Consequently, users who are familiar with MS-Windows do not have to learn several different command sequences for different applications. The features of MS-Windows include:

- Portability across computers running MS-Windows
- Multiple interactive windows for MS-DOS applications
- Access to Graphics Device Interface (GDI)
- Data exchange between applications
- Ease of use

Users who are unfamiliar with the MS-Windows interface can still execute MS-DOS commands at the DOS prompt.

• Network Applications Support

Digital's Network Applications Support (NAS) is a distributed, enterprise-wide computing strategy based on VAX, VMS, and DECnet/OSI technologies. Digital's PC integration products are a part of the NAS strategy. NAS allows customers to use a mixed set of systems, applications, and resources as a single, unified whole and has the ability to grow with future technological changes.

This spectrum of application sharing and networked communications is made possible by DECnet/OSI (Open Standards Interconnect). DECnet provides the communications protocols that allow different types of hardware and software equipment to interact almost seamlessly.

To meet customers' needs, Digital is tackling the difficult job of integrating Macintosh, MS-DOS, and OS/2 desktop architectures—in addition to VMS and UNIX—into LANs and WANs. Digital's strategy is to provide that integration with a single architecture using network application services on VAX systems and DECnet, and in compliance with open international standards. These services include applications access, business communications, and information resource sharing.

These features carry over into international applications as well. Digital is a leader in supporting international character sets to enhance usability of PCSA products worldwide.

▪ Standards

Digital's integrated personal computing products signal its renewed commitment to integrate enterprise-wide networks according to industry standards. To successfully integrate desktop systems from a wide range of vendors, Digital supports an open, industry-standard network. Digital believes that open networking standards are the best way for customers to implement a cohesive, distributed desktop computing strategy. Furthermore, Digital believes it is in the best interests of vendors and customers alike to formulate clear and open international standards.

Therefore, Digital supports the International Standards Organization's (OSI) standards for open networking. Digital's networking products will be OSI compliant, supporting worldwide standards for integrating equipment from multiple vendors.

Digital also supports open user interface standards. Digital, along with other desktop vendors such as Apple, supports the X Window standard and is committed to making the DECwindows user interface compliant with X Window standards. Digital's recent announcement with Apple included our joint commitment to continue to support OSI network and X Window standards.

▪ Other Resources

Further PCSA resources include various system support and maintenance services such as:

- DECsupport
- Basic and self-maintenance services
- Telephone hotline support for VAX/VMS Services for MS-DOS server and DECnet/PCSA Client software
- Training courses for end users and system administrators
- DECcompatible service on an array of selected non-Digital hardware that is connected to a VAX
- DECstart installation service, which is required when VAX/VMS Services for MS-DOS is installed initially

• PC Integration Products

Digital's PC integration products include the following:

- DECnet-DOS
- DECnet/PCSA Client: PC
- VAX/VMS Services for MS-DOS
- PCLAN/Server 2000
- Network Integration Kits
- Network Startup Kits

Trademarks

The following are trademarks of Digital Equipment Corporation: ALL-IN-1, DEC, DECcompatible, DECconnect, DECnet, DECnet-DOS, DECnet Scheduler, DECrouter 200, DECstart, DECsupport, DECsystem-10, DECSYSTEM-20, DECwindows, DELNI, DELUA, DEMPR, DEPCA, DEQUNA, DESPR, DESTA, DEUNA, the Digital logo, DNA, LA20, LA50, LA75, Letterprinter, Letterwriter, LN03, LN03 Plus, LN03R Scriptprinter, MicroVAX, Network Applications Support, PCSA Client, PCLAN/Server, PDP-11, PRO/DECnet, Professional, RSX, ThinWire, ULTRIX, VAXcluster, VAXmate, VAX/VMS, VMS, VT, WPS, WPS-PLUS/DOS.

Apple is a trademark of Apple Computer, Inc.

ASHTON-TATE is a trademark of Ashton-Tate Corporation.

COMPAQ DESKPRO Model 2 and COMPAQ DESKPRO 286 Model 40 and COMPAQ DESKPRO 386 Model 20 are trademarks of COMPAQ Computer Corporation.

Etherlink is a trademark of 3Com Corporation.

Hewlett-Packard is a trademark of the Hewlett-Packard Company.

Hewlett-Packard Ink Jet Printer is a trademark of the Hewlett-Packard Company.

HP is a trademark of the Hewlett-Packard Company.

IBM is a registered trademark of International Business Machines Corporation.

IBM Personal Computer, IBM Personal Computer XT, and IBM Personal Computer AT are registered trademarks of International Business Machines Corporation.

IBM Proprinter is a registered trademark of International Business Machines Corporation.

Lotus is a registered trademark of Lotus Development Corporation.

Macintosh is a trademark of Apple Computer, Inc.

MICOM-Interlan is a trademark of MICOM Systems, Inc.

MS is a trademark of Microsoft Corporation.

PC workstations that connect to the network and access large system services over the network are called *clients*. Using DECnet/PCSA Client software, clients can connect to a VAX or MicroVAX system by using asynchronous DECnet or Ethernet communications.

The server/client relationship is central to the PCSA network. Figure 1-1 is a conceptual drawing of this relationship of servers and clients on an Ethernet network.

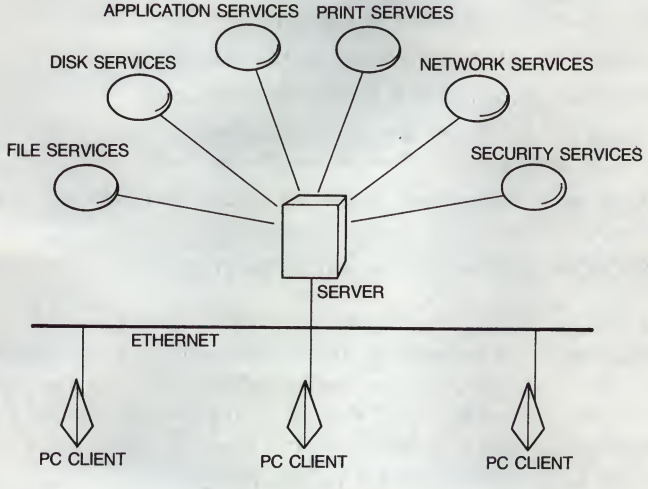


Figure 1-1 · PCSA Server/Client Relationship

· Servers

A *server* is any VAX or MicroVAX computer running PCSA server software. The server makes disks, printers, and other devices connected to the computer available to clients on the network.

For groups of PCs, servers provide the following: a central mass-storage facility; an easy way to share files, data, and applications; and a way to share peripheral devices such as printers and plotters. To the user, servers appear as additional local disk drives and printers.

Servers run the PCSA file and disk server software that sets up and provides remote file, disk, printer, and boot services to the clients in the network.

File Server

The file server provides file and print services to the PC workstation. Clients that use a file server run MS-DOS-based application software that is installed on a server as if it were installed on a PC. Data files also can be shared by the file server and manipulated as though they too were located on a PC's hard disk. The file server is a DECnet network application that allows clients to access directories and print queues on a VAX computer.

Setting up a VAX/VMS system as a file server involves several steps:

1. Installing the file service software on the VAX/VMS system
2. Registering PC workstations with the file server
3. Setting up the file services such as creating the common directory or personal directories for clients on the network
4. Assigning a service name to the file service for clients accessing the directory
5. Setting user read/write access to the directory

Disk Server

The disk server is a program that allocates space on a VAX/VMS disk where PCSA clients can create, store, and maintain MS-DOS files. This space, called a virtual disk, appears as a VAX/VMS file on the server and allows a client workstation to access it as though it were a local disk drive.

The disk server is implemented in three ways:

- LASTDRIVER, a device driver that interfaces to the VAX/VMS Ethernet driver and provides network transport between the PC workstation and the VAX computer
- LADDRIVER, a device driver that interfaces between LASTDRIVER and the VAX/VMS disk driver and provides the disk server functions
- LAD$KERNEL, a VAX/VMS process that controls access to the virtual disks

▪ Services

The services available to clients on a network are:

- File services, for access to directories and files stored on the server (available with VAX/VMS Services for MS-DOS in a LAN or WAN environment)
- Virtual disk services, for access to virtual system, application, and user disks
- Printer services, for network access to printers (available with VAX/VMS Services for MS-DOS in a LAN or WAN environment)

These services can be combined and used together.

File Services

The file service software stores MS-DOS files as standard Record Management System (RMS) files on the VAX/VMS server. MS-DOS data and application files can be specified as either stream or fixed-length, 512-byte records.

There are four types of file services:

- System directory
- Application directory
- Common directory
- User directory

The *system directory* contains PCSA system software. Clients share this software on the network.

The *application directory* contains executable files for MS-DOS applications that users can share (according to the licenses). In this way, one copy of the application software can be distributed to clients over the network.

The *common directory* contains data and text files that users can share and update.

The *user directory* contains user files.

Figure 1-2 shows an example of a file service.

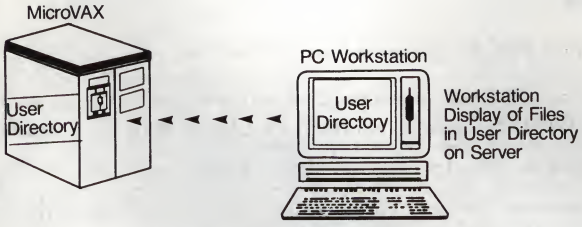


Figure 1-2 ▪ PCSA File Service

Virtual Disk Services

A virtual disk is a VAX/VMS sequential, fixed-length 512-byte record file that allows connections from PC workstations. To the server, the file is visible as a single VAX/VMS file. The MS-DOS files stored within the disk server are not visible as VAX/VMS files.

The virtual disk service sets aside space on a VAX/VMS disk for clients to access it as an MS-DOS virtual disk. The virtual disk is like an MS-DOS disk within a VAX/VMS disk, as shown in Figure 1-3.

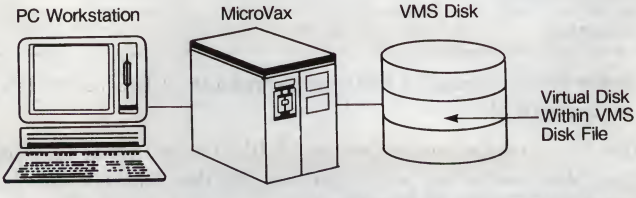


Figure 1-3 ▪ Virtual Disk on a VAX/VMS Disk

Users can create, maintain, and delete directories on the virtual disk using MS-DOS commands, just as they create, maintain, and delete directories on local diskettes or on a hard disk. The files stored on the virtual disks are MS-DOS data, system, or application files. The size of the virtual disk (up to 32Mb) limits the size of the files.

Because virtual disks allow either multiple-read or single-write access, virtual disks are well suited for either:

- Libraries of stable files that many users access for reference, such as applications files, system utilities, and development tools, or
- Personal directories that are not shared among users.

Virtual disks provide hard disk capabilities at less cost without loss of speed or productivity.

Because a virtual disk service bypasses the translator of the file service, the virtual disk can provide access to files and data more quickly than a file server.

Users also can access a virtual disk from a PC workstation using the asynchronous DECnet-DOS Network Device Utility (NDU). For information about the DECnet-DOS utilities, see *Chapter 9*.

To provide virtual disk service, mount the virtual disk. The virtual disk can be mounted temporarily or permanently. The virtual disk service is a VAX/VMS file that PC workstations can connect to through an MS-DOS drive. To the PC workstation, the virtual disk service is like any other MS-DOS disk and is assigned a drive letter as other MS-DOS disks. The drives appear local to the PC workstation.

After connecting to the virtual disk, users can move among the diskette, hard disk, and virtual disk drives by typing the disk drive identification letter or, from MS-Windows, by clicking on a drive icon. With MS-DOS commands, users can store, rename, copy, and delete files in the virtual disk directories and between directories on the virtual disk, hard disk, and diskette.

Local area disks (LADs) have the following characteristics:

- Compatibility with DECnet-DOS virtual disks
- Complementary with the file server
- Support for disk sizes 360Kb to 32Mb, for a total of 128Mb of storage per PC workstation
- Support for remote boot capability

Although a disk server does not differentiate among virtual disk services, four types of virtual disk services are useful for system management purposes:

- System virtual disks
- Application virtual disks
- Personal virtual disks
- Network key disks

System virtual disks contain the PCSA system software. The system administrator creates the system virtual disk when installing PCSA.

Application virtual disks store MS-DOS application software. In a network environment, the system administrator can copy application software to a virtual disk and offer it with read-only access to multiple PC workstations or write-only access to a single PC workstation.

An application virtual disk size depends on the size of the applications to be installed on the virtual disk.

Personal virtual disks store user-specific data. Normally these disks are mounted for a single user and require a password for access. A user cannot share data stored in a personal virtual disk with VAX/VMS applications.

Network key disks are used to remote boot the PC workstation (start the MS-DOS operating system over the network). A network key disk is similar to a key diskette, except that the network key disk resides on the network rather than in a PC workstation's diskette drive or on the hard disk.

File Services Versus Disk Services

From the user's perspective, there is little difference between accessing file services or disk services. File services and disk services both appear as MS-DOS drives. File services are assigned to any drive. Disk services are assigned to specific drives, depending on the PC workstation configuration.

You can configure MS-DOS PC workstations that optimize performance and functionality through the use of both servers. For example, place all system software on a system virtual disk and place application software on one or more application virtual disks. Users should access private data files through the file server using a personal account and shared data files through the file server using common file service.

Table 1-1 lists the differences between a file service and the disk service.

Table 1-1 • File Versus Disk Services

Capability	File Service	Disk Service
Shared read/write access	Yes	No
Files accessible from MS-DOS and VAX/VMS	Yes	No
WAN access	Yes	No
Remote boot available for PC workstations	No	Yes

In most cases, the disk server also provides faster access to MS-DOS files than the file server does. Table 1-2 shows which server would best meet users' needs based on what type of work they are doing.

Table 1-2 ▪ When to Use the File Server or the Disk Server

Server	Usage
Disk server	For files that users access read-only. Simultaneous users have fast access to read-only disks. For example, if you store an application with the disk server, multiple users can access the application quickly.
File server	For files that users access with both MS-DOS and VAX/VMS. Files stored with the file server are visible to RMS as VAX/VMS files. For example, if you share your WPS-PLUS files between MS-DOS and VAX/VMS, you must store them in a file server directory so WPS-PLUS/VMS will recognize them.
File server	For files that users access read and write simultaneously.
Disk server	For files that users access read and write one user at a time.

Printer Services

A printer service is a print queue on a VAX computer that a PC workstation can access. PC workstations can spool an MS-DOS file to a VAX/VMS printer queue. The file server directs the file to a spool file and queues a spool file to a VAX/VMS print queue.

Printer services allow users to connect to and use printers connected to a VAX/VMS server or VAXcluster in either a LAN or WAN environment. Users can send data or graphics from MS-DOS, MS-Windows, or applications to the printer service as shown in Figure 1-4.

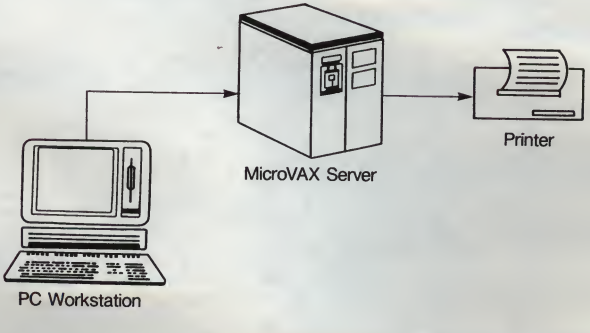


Figure 1-4 ▪ PCSA Printer Services

The system administrator is responsible for setting up remote printing for the printer services according to the operating system in use.

On a VAX/VMS server, the system administrator does the following:

- Creates a VAX/VMS print queue
- Defines forms for the VAX/VMS print queue
- Assigns a service name to the printer services
- Defines user access to the printer services

▪ Clients

A network running the VAX/VMS Services for MS-DOS software supports Digital and selected non-Digital PC workstations running DECnet/PCSA Client software. Clients are connected to ThinWire Ethernet using a Digital Ethernet Personal Computer Adapter (DEPCA) or other supported third-party Ethernet controller boards. Clients can also be integrated into the PC LAN using asynchronous communications.

For a list of supported Ethernet controller boards, see the Software Product Description (SPD) 55.07.XX.

PC workstations can use local printers, files, applications, and other local resources that are available to the PC workstation as a standalone PC. More importantly, you can connect PCs to the network as clients to use printer services, file services, and virtual disk services, and to share files and applications available from servers on the network.

Each client in the network can use resources connected directly to the PC workstation (local) or the resources available as services from a server (remote). The clients request use of a service and the server responds to, or serves, the requests. The client uses the service as if it were local.

Chapter 2 · Hardware Configuration

PCSA is an open-ended architecture that supports multiple configurations. The range of options meets the needs of various network topologies. This chapter explains which PCs are supported, how they are networked, and gives an example of how they could be configured.

· Supported Third-Party Hardware

Besides supporting the IBM Personal Computer, IBM Personal Computer XT, and Personal Computer AT, PCSA supports other hardware:

- COMPAQ DESKPRO Model 2, COMPAQ DESKPRO 286 Model 40, and COMPAQ DESKPRO 386 Model 20
- IBM PS/2 Model 30, 50, 60, and 80 (both Ethernet and asynchronous DECnet communications)
- IBM (Personal Computer XT and AT, Enhanced, PS/2) and COMPAQ keyboards
- Olivetti M24, M28, M240, M280
- Zenith 248

PCSA will also support additional vendors' PCs after they are tested and approved. For the current list of supported PCs, refer to the SPDs.

· Connecting PCs to a Server

PC workstations connect to servers using either asynchronous or Ethernet communications. PC workstations require that either the Digital Ethernet Personal Computer Adapter (DEPCA) controller board or one of the supported Ethernet controller boards, such as a 3COM or MICOM-Interlan Ethernet board, listed in the Software Product Description (SPD 30.50.XX) is installed.

In addition to using selected third-party Ethernet cards, you can network standalone PCs by adding the components of Digital's Network Integration Kit. In addition to a Digital keyboard and mouse, the PC workstation Network Integration Kit provides a DEPCA board required to connect the PCs to an Ethernet network. The DEPCA is available with either a ThinWire Ethernet cable assembly or a standard Ethernet cable assembly.

Each Network Integration Kit includes the following components:

- DECnet/PCSA client license
- DEPCA board
- ThinWire Assembly Kit (with ThinWire Ethernet cables, T-connectors, and terminator)
- Digital mouse (DEPCA-K kit only)
- Digital keyboard (DEPCA-K kit only)

When connecting a PC workstation with a controller other than a DEPCA, refer to the Ethernet controller hardware documentation for information on configuration and switch settings.

To connect a PC workstation using asynchronous DECnet to a PCSA network, install an asynchronous communications controller in the PC workstation.

For further information, refer to the *DECconnect System Planning and Configuration Guide.*

▪ Digital Ethernet Personal Computer Adapter

The Digital Ethernet Personal Computer Adapter (DEPCA) is an Ethernet communications controller that connects the IBM Personal Computer—IBM Personal Computer XT, IBM Personal Computer AT, or IBM-compatible—to the Ethernet LANs as clients. The DEPCA connects directly to ThinWire Ethernet cable, using integral transceiver circuitry. With the addition of the DEPCA-AU connector option, the DEPCA can connect to standard baseband Ethernet cable by means of an Ethernet transceiver or local Network Interconnect (NI).

The DEPCA is available with either a ThinWire Ethernet cable assembly or a standard Ethernet cable assembly [Attachment Unit Interface (AUI)].

Digital supports 3COM Etherlink II, Etherlink/MC, and MICOM-Interlan NI5010-1 and NI5010-2 third-party Ethernet controller cards. However, DEPCA provides advantages over some non-Digital Ethernet controllers because it has support for a high-performance architecture to work with VAX/VMS servers (the Etherlink II is also multibuffered). Only Digital's DEPCA provides the ability to boot PC workstations from a network key disk.

The DEPCA memory buffers allow for efficient, high-speed communications with a VAX computer. Other single-buffered Ethernet controllers must immediately process any data as it is received. During processing, any additional data sent to the PC workstation can be lost, requiring the VAX computer to retransmit the data. This constant retransmission of data can affect both PC workstation and server performance. When communicating with a VAX computer, the DEPCA can process the initial data received and buffer any addi-

tional data received. Little data is lost, so fewer retransmissions are required. In this way, the DEPCA provides increased performance over other Ethernet controllers in a DECnet network.

With the DEPCA, users can boot their PC workstations using network key disks. A network key disk is a virtual disk that a PC workstation uses to remote boot. Other Ethernet controllers do not provide the same capability.

The DEPCA board allows the system administrator to change the jumper settings to match the PC workstation. This added versatility makes the DEPCA compatible with a combination of PCs and user-supplied options. The jumpers control memory size and address, I/O address, interrupt vector for the network interface and mouse, and ThinWire or standard Ethernet assignment. The system manager can select boot and IEEE 802.3-compliant grounding for the AUI option connector.

The function of jumpers W7, W8, and W16 depends on the DEPCA board revision level and the version of DECnet-DOS software used.

The revision level code is on a bar code label on the back left corner of the DEPCA board. Only the first letter of this two-character code is significant. This label is below the nine-digit part number label shown in Figure 2-1.

DEPCAs revision E (or later) are compatible with all versions of DECnet-DOS software. However, to use the 32Kb mode on DEPCA revision E, the system must be running DECnet-DOS V2.1 or later.

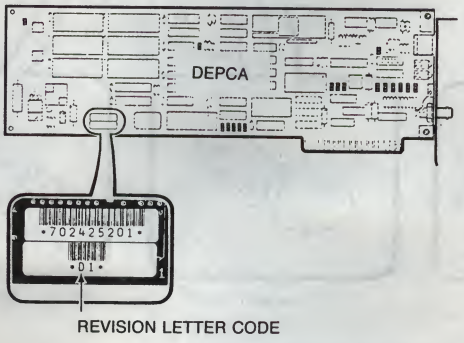


Figure 2-1 ▪ DEPCA Board Revision Level

The DEPCA board has 17 jumpers so that it is compatible with IBM Personal Computers. The locations of the jumpers are shown in Figure 2-2. The DEPCA board comes with all jumper settings already selected (default settings).

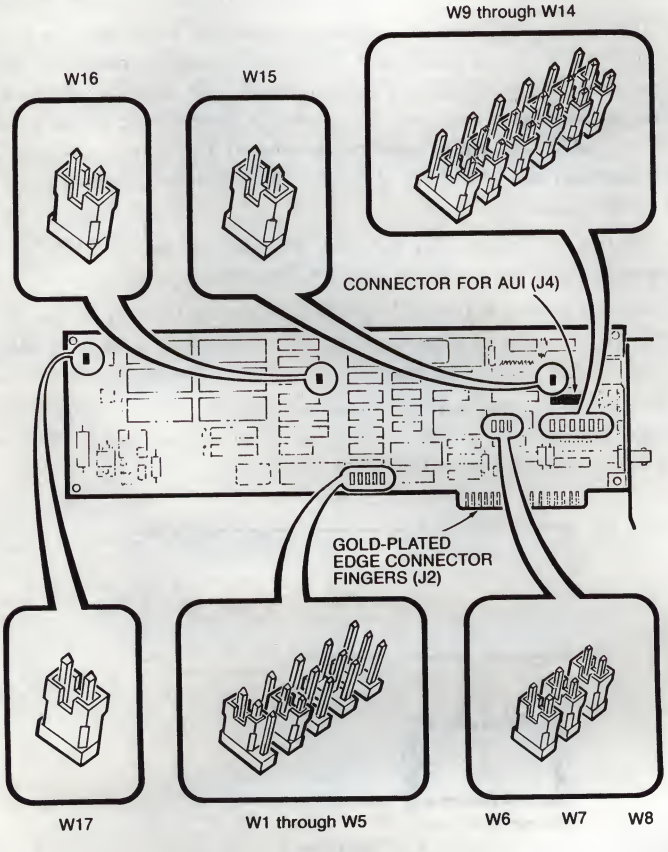


Figure 2-2 ▪ DEPCA Board Jumper Locations

Figure 2-3 shows the possible jumper settings. They include the following:

- No connection. The jumper is removed. Save the removed jumper for future use by sliding one side of the jumper on a single jumper pin (see Figure 2-3).
- Top connection. The jumper is installed on the top and center pins. The top pin in a row of three is the pin farthest away from the gold-plated card-edge connector.
- Bottom connection. The jumper is installed on center and bottom pins. The bottom pin in a row of three is the pin closest to the gold-plated card-edge connector.

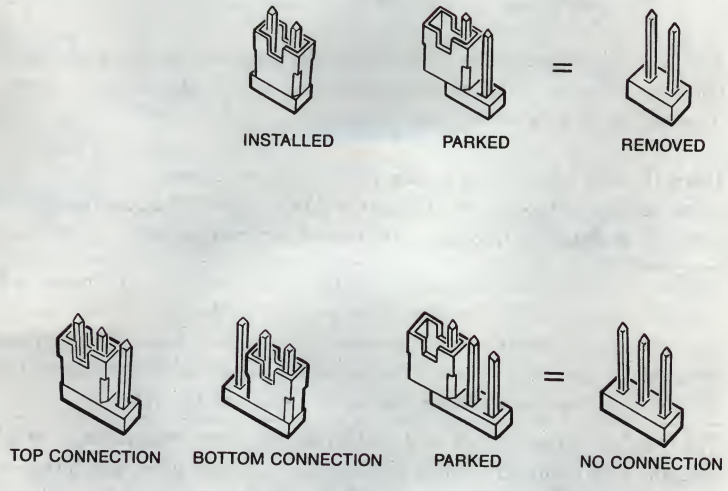


Figure 2-3 ▪ DEPCA Board Jumper Settings

▪ Asynchronous Communications

If a PC workstation does not have access to Ethernet—the station is in a remote office, for example—the PC can connect to a file server using asynchronous communications. PCSA is designed to run with both Ethernet and asynchronous communications. Since asynchronous communication does not provide the high-speed performance of Ethernet, it is recommended that only casual users run PCSA using asynchronous communications. Table 2-1 compares the PCSA services available using Ethernet versus asynchronous communications.

Table 2-1 ▪ Ethernet Versus Asynchronous Services

Service	Ethernet	Asynchronous
Remote file services	Yes	Yes
Remote printer services	Yes	Yes
Virtual disk services	Yes	Yes (NDU only)
Boot using network key disk	Yes	No
Terminal emulation	Yes (LAT and CTERM)	Yes (CTERM only)

The physical connection to a VAX/VMS host computer can be made one of two ways, either using a serial communications port for asynchronous communications, or directly through the Ethernet.

Using the File Server with Asynchronous Communications

There are two methods for setting up the VAX computer to accept connections from PC workstations through asynchronous communications:

- Digital recommends connecting to a DECrouter 200. The DECrouter 200 should be connected to the same Ethernet LAN as the PC workstations that are running asynchronous communications. This method reduces the overhead incurred by the VAX computer in servicing the asynchronous lines. This method only requires a DECnet end node license on the VAX.
- The PCs can connect directly to the VAX computer through serial lines. In this case, the VAX computer must be configured as a routing node, which requires a full-function DECnet-VAX license. The serial lines can be either dedicated DECnet lines or dynamically switched terminal lines to DECnet.

A dynamically switched terminal line is a terminal line that the user can switch to a DECnet Digital Data Communications Message Protocol (DDCMP) line.

Both types of lines can connect to the VAX computer through a modem or hardwired directly to the VAX computer.

DECrouter 200

The DECrouter 200 is a software/hardware server that runs on a dedicated hardware base to provide the DECnet routing functions for up to eight DECnet nodes connected to the asynchronous DDCMP connections. These nodes can be IBM Personal Computers or IBM compatible running DECnet-DOS or other Phase III or Phase IV DECnet nodes using asynchronous DDCMP DECnet connections.

The DECrouter 200 is also connected to the Ethernet and provides access to the Ethernet (and the wider DECnet network) and to the nodes attached to the asynchronous ports. The nodes attached to the asynchronous ports may be located either locally, by dedicated wiring such as existing office wiring, or they may be located remotely by modem connections.

The DECrouter 200 can off-load the routing-related communications processing load from the host, thereby freeing up host processor and memory resources. The DECrouter 200 also performs the routing functions on the Ethernet that allow end nodes not directly connected to the Ethernet to communicate with Phase IV hosts directly connected to the Ethernet.

▪ DECconnect Communications System

The DECconnect communications system encompasses the full family of Digital products from network electronics to cabling and connections. DECconnect provides access to corporate computer networks, telephone communications, and a video network. The modular nature of DECconnect lets the user mix and match components to meet specific requirements.

DECconnect offers a simple, cost-effective cabling system that brings both high-performance baseband Ethernet and enhanced EIA 423-A terminal connection to office and work areas. Through separate, industry-standard cabling runs that radiate from a centralized equipment/wiring area (called the satellite equipment room) to an integrated faceplate in the work area, DECconnect cabling allows a customer to connect terminals, PCs, and workstations. With standard Ethernet cable as a backbone, users have access to data center and mainframe resources.

ThinWire Ethernet Cabling

ThinWire Ethernet cabling is an inexpensive, industry-standard coaxial cable with BNC connectors. This cabling enables the configuration of low-cost LANs in the work area. Like standard Ethernet coaxial cable, ThinWire cable delivers 10Mbps of Ethernet performance. ThinWire cable is designed specifically for horizontal wiring of a work area because of its easy installation and lower cost.

In the DECconnect communications system, ThinWire cable runs from a ThinWire Ethernet repeater in a satellite equipment room to DECconnect faceplates in a local work area. PC workstations are connected to the faceplates.

Unshielded Twisted-Pair Adapter

The unshielded twisted-pair Ethernet adapter delivers 10Mbps Ethernet performance to a remote PC workstation using up to 70 meters (164 to 230 feet) of twisted-pair building cable. The unshielded twisted-pair Ethernet adapter connects either a PC workstation equipped with a DEPCA or a PC workstation equipped with a compatible Ethernet controller to a Digital Ethernet Multiport Repeater (DEMPR).

The unshielded twisted-pair Ethernet adapter consists of two components: an unshielded twisted-pair office adapter and an unshielded twisted-pair wiring closet/SER adapter. They operate together to match the 50-ohm impedance on a ThinWire Ethernet cable to the impedance of an unshielded twisted-pair cable. Figure 2-4 shows a typical unshielded twisted-pair Ethernet configuration.

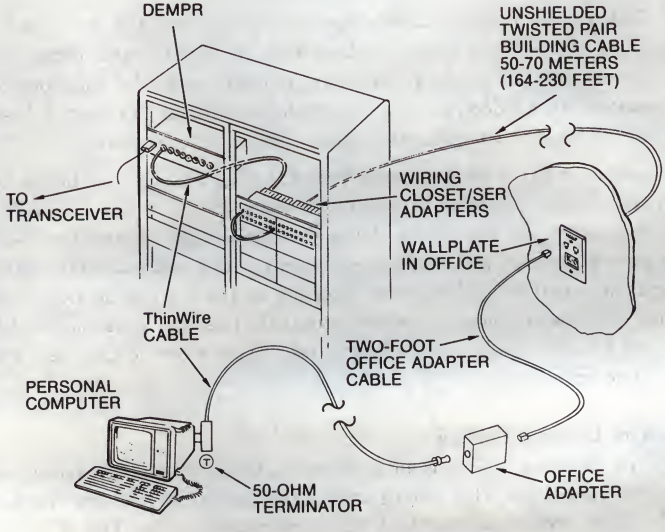


Figure 2-4 ▪ Unshielded Twisted-Pair Ethernet Adapter Configuration

Configurations with the DECconnect System

The simple yet flexible network configuration strategy of DECconnect creates an optimal network environment for installing PCSA servers and clients.

The DECconnect faceplate provides a single connection point for PC workstations and other office automation equipment. ThinWire Ethernet coaxial cable can be connected directly into the DECconnect faceplate. The faceplate makes it easy for a network user to make network connections for PC workstations, terminals, telephones, and video and communications equipment. If the user changes offices, no new rewiring is necessary. Figure 2-5 illustrates a faceplate connection.

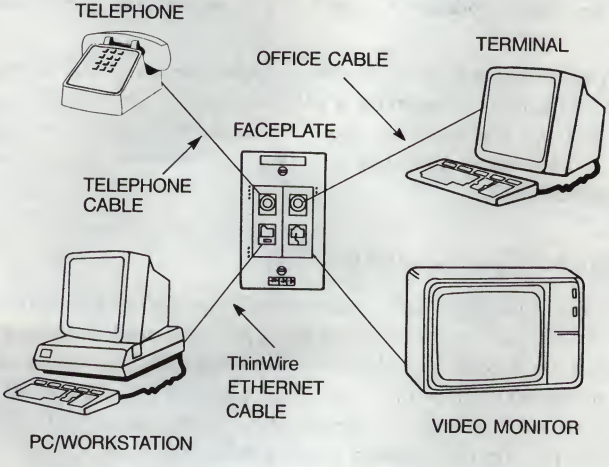


Figure 2-5 ▪ Faceplate Connection

Network Configurations Without DECconnect

PCSA network configurations can be installed easily in buildings that do not have a DECconnect System installed. Instead of connecting to a DECconnect faceplate, PC workstations connect from one to another and then to a server in a daisy chain, or each connects directly to a server. If a building's network configuration is upgraded to the DECconnect system, DECconnect PCSA configurations and non-DECconnect PCSA configurations can be integrated.

The PC workstations connect to each other using ThinWire cable attached to T-connectors that plug into the back of each PC workstation, thus creating a daisy chain of PC workstations. The first PC workstation in the chain connects through a Digital Ethernet Station Adapter (DESTA) to a VAX or MicroVAX computer. Each PC workstation in the chain has an incoming ThinWire Ethernet cable and an outgoing ThinWire Ethernet cable. The last PC workstation in the chain has an incoming ThinWire Ethernet cable and a terminator on the T-connector.

The server computer connects to the local network with transceiver cable. The DESTA connects the transceiver cable to the ThinWire Ethernet cable used by the PC workstations.

In addition to PC workstations, terminals and printers also connect directly to the server computer.

System administrators should prepare a complete network installation analysis before configuring and installing a LAN, especially when installation is in an older building. The office area must be planned to accommodate the PCSA server and PC workstations. Digital network specialists are available to assist with network planning.

▪ VAXcluster Considerations

VAX/VMS Services for MS-DOS can be installed on VAXcluster configurations. However, the network characteristics and DCL command tables only can be modified on the node where VAX/VMS Service for MS-DOS was installed. To make modifications from all cluster nodes, you must either reboot each node in the cluster, as described in the *VAX/VMS Services for MS-DOS Installation Guide*, or perform the following steps on each node in the cluster:

1. Set DECnet objects.
2. Define the PCSA command on each node (assuming that the initial definition is contained in the shared DCL tables).

File Servers in a VAXcluster

When a PC workstation opens a file, the file server puts a private lock on the file. If a second file server in the cluster attempts to access the same file with an incompatible access mode, the second file server routes PC workstation requests through a DECnet link to the file server that owns the lock. This file server arbitrates access to the file for all PC workstations.

In a VAXcluster, the file server supports MS-DOS byte-range locking. When offering a service on multiple nodes in a VAXcluster, each file server ensures that access to the file is coordinated through a single file server in the cluster.

If multiple PC workstations frequently update a file, they should all connect to the same node in the cluster. To maintain reasonable file server performance, PC workstations should access the service through a common file server.

In a VAXcluster, use one service database for all nodes, unless some services are restricted to specific nodes. In this case, use a service database for each node in the VAXcluster.

When running in a VAXcluster, store the log file in a special file so that the system manager knows which server produced the log.

Disk Services in a VAXcluster

The disk server can run on a VAXcluster and offer a disk for write access any time. If a second disk server in the VAXcluster subsequently tries to mount the disk with write access, it is mounted as pending. The subsequent request to mount the disk is not completed until the first disk server dismounts the disk.

If the disk has read access, it can be offered on multiple nodes in the VAXcluster with service connections distributed between nodes. The disk server's service database resolves conflicts when a disk is offered on multiple nodes in a VAXcluster. Only one copy of the database file should exist in a VAXcluster. The database file must be stored on a disk accessible to all nodes in the VAXcluster executing the disk server.

If the disk server in a local area VAXcluster is not running on the boot node, the disk server logicals (except the service database logical) should be redefined. These logicals should point to the local disk on the node running the disk server.

▪ Sample Configuration

This section provides sample hardware configurations for both DECconnect and non-DECconnect environments. Individual configurations differ depending on the needs and the network. The sample configurations in Figure 2-6 use specific network hardware, which is listed and defined in the *Glossary*.

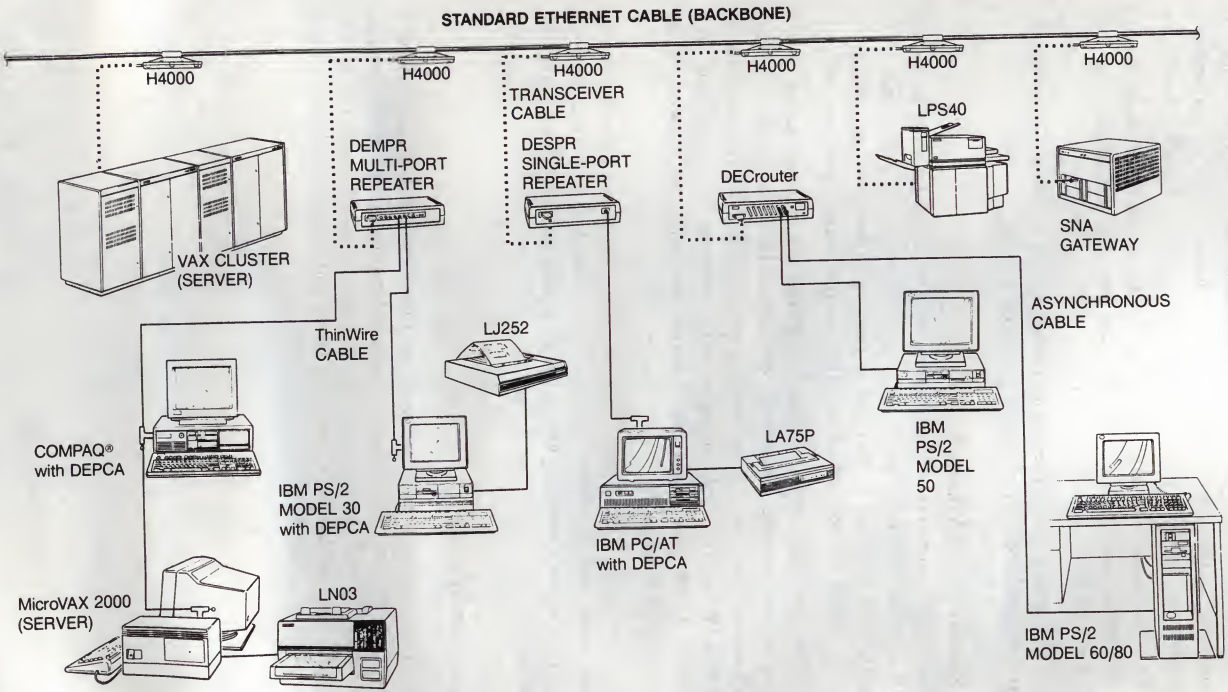


Figure 2-6 ▪ Sample PCSA Configuration

VAX/MicroVAX Server

Hardware
- DEPCA-RA Starter Kit for MicroVAX 2000 Server OR DESVA-AA ThinWire Ethernet Controller
- DEPCA-SA Starter Kit for MicroVAX II Server OR DESTA-AA For adapting a standard Ethernet controller to ThinWire

Software
- DECnet-VAX license (included in DEPCA-RA/SA): includes VAX/VMS Services for MS-DOS license
- Q*A93-H* VAX/VMS Services for MS-DOS media/documentation

Service
- QS938-SZ PCSA DECstart (first server installation only)
- Q*A93-** DECsupport, Basic, Self-maintenance

PC Options
- N/A

VAXmate Client

Hardware
- PC500-BA (green)
- PC500-CA (amber)
- Includes DECnet/PCSA Client: VAXmate license

Software
- Q6ZP3-UZ DECnet/PCSA Client license[2] (one required per PC; included with PC500 since February 1988)
- Q6ZP3-H* DECnet/PCSA Client: media/documentation (one copy per network)

Service
- Q6ZP3-3*/3Z Self-maintenance/Service-Right-to-Copy

PC Options
- PC50X-AA 2-MB RAM
- FP287 Math Coprocessor
- PC50X-MA Modem
- RCD3*-FC Expansion Box with Hard Disk

Selected Compatibles Client

Hardware
- DEPCA-KA/DEPCB-V* IBM PC Network Integration Pkg OR DEPCA-BA/DEPCB-B* PC Network Services Pkg[2] (Both packages include QBZP3-UZ DECnet/PCSA Client: PC license) OR A supported third-party Ethernet controller[1] OR Asynchronous support

Software
- QBZP3-U* DECnet/PCSA Client: PC license[2] (one required per PC; included in DEPCA-KA/BA)
- QBZP3-H* DECnet/PCSA Client: media/documentation (one copy per network)

Service
- QBZP3-3*/3Z Self-maintenance/Service-Right-to-Copy

PC Options
- DEPCA-AU (For direct connection to standard Ethernet backbone)
- VSXXX-AA Corporate Mouse

PS/2 Models 50/60/80 Client

Hardware
- Asynchronous support OR A 3C523 Etherlink/MC Ethernet Multibuffered controller

Software
- QBZP3-UZ DECnet/PCSA Client license[2] (one required per client)
- QBZP3-H* DECnet/PCSA Client: media/documentation (one copy per network)

Service
- QBZP3-3*/3Z Self-maintenance/Service-Right-to-Copy

PC Options
- N/A

* Denotes variant fields. Refer to the appropriate price book.
[1] Refer to SPD 55.07 for supported configurations.
[2] Quantity pricing available.

The sample configuration in Figure 2-7 uses specific network hardware, which is listed and defined in the *Glossary*.

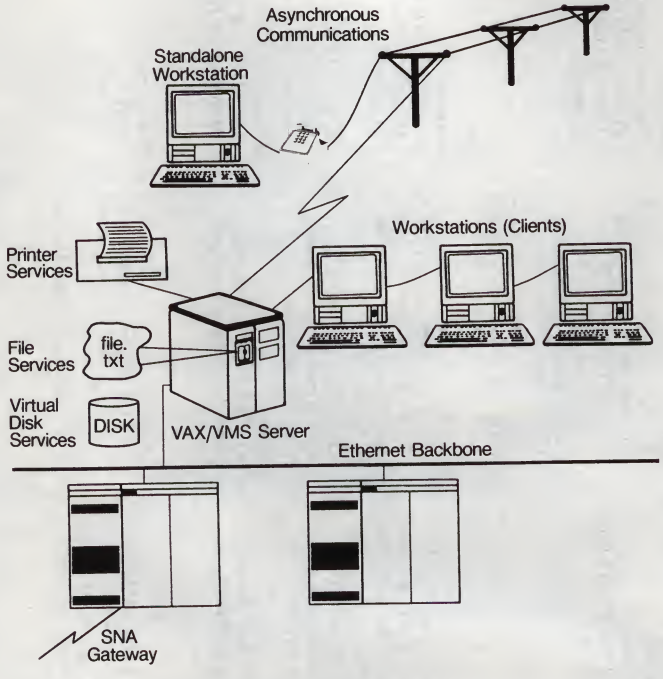


Figure 2-7 ▪ A Simplified Network

▪ Digital PCLAN/Server 2000 Configuration Option

The PCLAN/Server 2000 is a complete configuration solution for the small office environment. Using a customized MicroVAX 2000 as the server, it offers a low-end (8 to 30 users) local area networking solution to isolated work groups. Because of compliance with the PCSA strategy, it also becomes a building block for the thorough integration of PCs into the larger corporate network.

The maintenance and configuration functions can be done either at a Digital Command Language (DCL) level or by using the menu-driven setup program. This means that the system administrator need not be familiar with the VAX/VMS operating system.

The PCLAN/Server 2000 configuration package includes the following:

- MicroVAX 2000 with 4Mb of memory
- 1.2Mb RX33 floppy
- Ethernet controller
- Expansion adapter
- VT320 Console (for administrative purposes)
- Tape media/backup (TK50 95Mb)
- 159Mb RD54 hard disk drive
- Four serial ports
- VAX/VMS single user license
- DECnet-VAX end node license
- Bundled client license for PCs
- DECnet enhanced support of MS-NET, MS-Windows, MS-DOS
- PC-MAIL with Sensitive Digital text editor (SEDT) application
- Packaged tape/disk media and documentation kit

The PCLAN/Server 2000 provides simplified network planning, implementation, and management. The straightforward, flexible integration architecture allows the system to grow with the group. Figure 2-8 shows how the PCLAN/Server 2000 configuration can act as the building block for a corporate network.

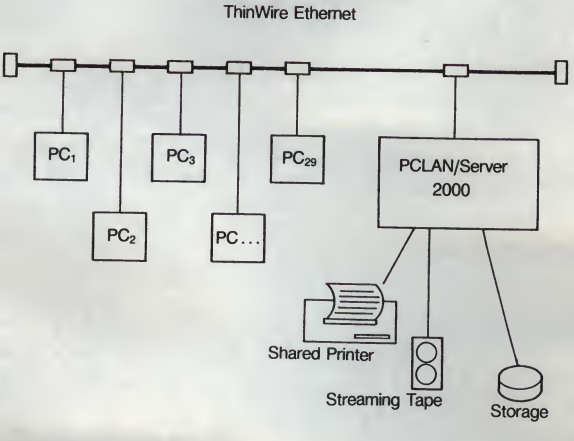


Figure 2-8 ▪ Using PCLAN/Server 2000 as a Building Block

Chapter 3 • Managing the Network

Once a network is running, the system administrator ensures that it continues to run smoothly. To simplify this task, the PCSA software contains network management utilities. These utilities allow the system administrator to configure PC workstations, manage the virtual disk, and add printer services.

• VAX/VMS Services for MS-DOS

VAX/VMS Services for MS-DOS software is a DECnet application. It implements PCSA, allowing VAX and MicroVAX computers to act as application, data, and resource servers to groups of PCs. By using these server systems, PCs can share applications, data, and resources; access information from remote systems on the network; and apply that information in MS-DOS applications.

VAX/VMS Services for MS-DOS software provides a complete range of services to allow management and control of the network. Access to network file, disk, and print resources can be limited by the use of passwords and VAX/VMS Access Control Lists (ACLs). The system administrator also can monitor and control each user account and collect valuable information on network activity to help meet performance and security goals. PCSA client accounts can be changed easily as their needs change.

VAX/VMS Services for MS-DOS provides the following services for personal computers running DECnet/PCSA Client software:

- File services
- Disk services
- Print services
- Time and date services
- Server management and control

Upgrading to VAX/VMS Services for MS-DOS V2.0

If you are currently running VAX/VMS Services for MS-DOS V1.0, use the complete V2.0 media and documentation kit to upgrade to V2.0. The procedure is similar to that for installing V2.0. However, you should also upgrade the file services (PCAPP, VXSYS, and applications, for example). Personal services do not need to be upgraded.

The PCFS_UPGRADE.COM utility allows you to upgrade file services from previous versions.

Before upgrading VAX/VMS Services for MS-DOS be aware of the following:

1. You must be logged into the SYSTEM account to run PCFS_UPGRADE.
2. Note that the upgrade procedures delete all files in the system directory structure (VXSYS.DIR or ISSYS.DIR). Back up any non-Digital files that you might have copied to the directory structure before upgrading the file server.
3. When upgrading the file server from V1.x to V2.0 using PCSA_UPGRADE, add the printer queue using the PCSA_ADMIN utility. Ignore any error messages you receive. This procedure creates a corrected PCFS_PRINT.COM file.

▪ Remote Boot Capability

One of the key features of the PCSA software is its ability to boot a PC workstation from a virtual disk called a network key disk. Known as remote boot, this procedure takes advantage of the virtual disk's fast performance.

To configure the PC workstation for remote boot the following conditions must be met:

- The PC workstation must have a DEPCA board.
- The server must be a VAX/VMS computer.
- The network key disk must be either 360Kb or 1.2Mb.

Figure 3-1 shows the sequence of a remote boot procedure.

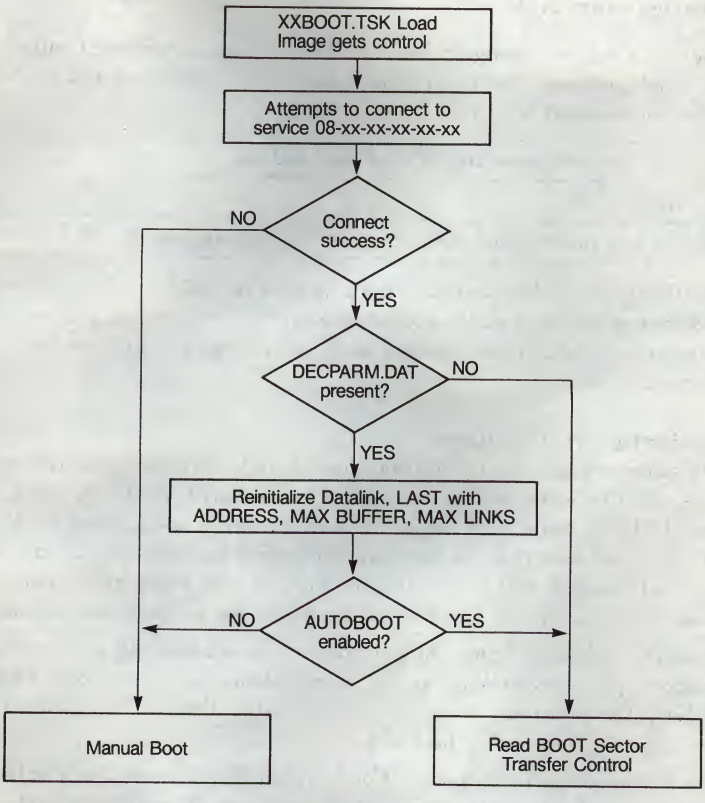


Figure 3-1 ▪ Remote Boot Sequence Flowchart

▪ PCSA Administration Utility

The PCSA Administration Utility (PCSA_ADMIN) is created when the DECnet/PCSA Client software is installed. PCSA_ADMIN stores data files used to administer and manage users on the network. The PCSA_ADMIN service also contains a database file that defines remote application directories used in the creation of a user profile.

▪ Configuration Aide

The system manager configures each user's PC workstation with the Configuration Aide program. This program runs under MS-Windows and collects the following information for each PC workstation:

- PC's DECnet node name and DECnet node address
- PC type
- Applications, printers, and directories that the user accesses

The Configuration Aide also maintains a database of DECnet node names and addresses as well as a database of applications on the network. The system manager can update these databases when an application or DECnet node is changed.

Configuring a PC Workstation

The system manager can use the Configuration Aide to configure PC workstations. The Configuration Aide creates the files necessary to boot a PC workstation. If the PC workstation has a hard disk, the system manager can run the Configuration Aide from the user's PC workstation and copy files directly to the hard disk. The preferred method for booting a PC workstation is remote boot. The boot files are stored on the server and not on the PC workstation.

If the PC workstation being configured does not have a hard disk or is not the current type of PC workstation, the system administrator can create a key diskette. Users then use the key diskettes to start up their PC workstations or they copy the files to their hard disks.

The system administrator uses the Configuration Aide to create the four files used to boot the PC workstation. Two of the files are PC workstation profiles and two are user profiles. Profile files contain specific configuration information for a particular PC workstation or user. The file names created by the Configuration Aide are:

- CONFIG.SYS—PC workstation profile
- AUTOEXEC.BAT—PC workstation profile
- AUTOUSER.BAT (USER.BAT)—User profile
- WIN.INI—MS-Windows initialization file

The PC workstation profiles are separated from the user profile to allow multiple users to share a single PC workstation. In addition, any one user can work on more than one PC workstation.

The CONFIG.SYS file contains PC workstation-specific information, such as the device drivers that are loaded for the PC workstation. The file loads automatically when the user boots the PC workstation.

The AUTOEXEC.BAT file contains PC workstation-specific information for using the PC workstation as a PCSA client. The file contains hardware and configuration information about the PC workstation:

- The PC workstation node name and address
- The location of the system directory the PC workstation accesses
- The kind of Ethernet controller board used by the PC workstation
- Whether the PC workstation can be used for MS-Windows
- Country-specific information, such as the country name and character set type
- Optional devices or commands to be added to the PC workstation configuration file
- The network switches for PC workstation use

When a user boots a PC workstation the AUTOEXEC.BAT file runs and configures the PC workstation. After the file completes processing it does one of two things:

- Issues an AUTO-LOGIN command to run the AUTOUSER.BAT file automatically, or
- Prompts the user to log in at the MS-DOS prompt and then it connects to the service where the AUTOUSER.BAT file is stored. Once the connection is made, the AUTOEXEC.BAT file is executed.

The AUTO-LOGIN command is useful when one user always works at the same PC workstation. Requiring the user to log in at the MS-DOS prompt means that more than one user can boot and use the same PC workstation.

The AUTOUSER.BAT file contains information about the user's working environment. This file name appears as USER.BAT on a key disk or diskette. The file contains information about the following:

- Connections to remote printers
- Connections to file services
- Connections to virtual disk services
- Connections to user directories (either a common or application directory)
- Directories to add to the MS-Windows search path

- Directories to add to the MS-Windows application append path for application-specific files
- Optional startup commands to add to the AUTOUSER.BAT file
- Whether MS-Windows or MS-DOS starts as the user interface

The WIN.INI file contains information about how the user works with MS-Windows. The WIN.INI file includes:

- Any application the system starts with MS-Windows
- Any application to load as icons when MS-Windows starts
- Additions to the file extension mapping list

The system administrator stores the CONFIG.SYS and the AUTOEXEC.BAT files on the server, a key diskette, or a network key disk for each PC workstation. The user profiles also can be added to the key diskette or network key disk.

▪ Managing the Virtual Disk

The system administrator is responsible for creating and maintaining the virtual disk on the VAX or MicroVAX computer. The system administrator's tasks include:

- Installing the virtual disk software on the VAX/VMS system
- Setting aside blocks on the VAX/VMS disk for each virtual disk
- Registering PC workstations with the virtual disk server
- Setting user read/write access to the disk
- Making virtual disks available to users
- Maintaining disks, including monitoring traffic and use, so the disks are not overloaded
- Performing backups of the data stored on the virtual disks

The system administrator uses the PCSA_MANAGER utility to set aside blocks on the VAX/VMS disk for a virtual disk. The size available for the virtual disk is variable and can be set and changed using PCSA_MANAGER.

The system administrator configures a user's PC workstation as a client and assigns MS-DOS drive identification letters to the virtual disk. To MS-DOS, the virtual disk looks like a diskette.

Drive Allocation

When the PC workstation is booted from a key disk, the software allocates drives and connects them to specific resources (directories, files, and printers) on a server. The AUTOEXEC.BAT and AUTOUSER.BAT files assign drive letters to resources a user can access. The software reserves certain drives based upon several factors:

- Number and type of physical devices connected to the PC workstation
- Number of hard disk partitions on the PC workstation
- Order in which device drivers appear in the CONFIG.SYS file

Table 3-1 shows the devices for which drives are allocated and the sequence of their allocation for V2.0 of PCSA. The table divides PC workstations into those with hard disks and those without.

Table 3-1 ▪ Drive Allocations for V2.0 of PCSA

Drive Letter	Without Hard Disk	With Hard Disk (One Partition)
A:	Diskette drive 1	Diskette drive 1
B:	Diskette drive 2	Diskette drive 2
C:	Virtual disk drive 1	Hark disk
D:	Virtual disk drive 2	Virtual disk drive 1
E:	Virtual disk drive 3	Virtual disk drive 2
F:	Virtual disk drive 4	Virtual disk drive 3
G:	Unused or RAM disk	Virtual disk drive 4
H:	Unused	Unused or RAM disk
I:	Unused	Unused
J:	Unused	Unused
K:	Unused	Unused
L:	System directory	System directory
M:	Personal	Personal
N:	Common	Common

Table 3-1 •Drive Allocations for V2.0 of PCSA (Continued)

Drive Letter	Without Hard Disk	With Hard Disk (One Partition)
O:	Unused	Unused
P:	Reserved for administrative service when running the Configuration Aide	
Q:–Z:	Drives can be used to connect to application services and shared databases.	

If the hard disk has more than one partition, the first virtual disk drive moves down one drive letter. A PC workstation configured with the Configuration Aide can have a maximum of four partitions on the hard disk.

Application Service

The application service contains software for applications. The service is created with VAX/VMS Services for MS-DOS. The application can then be installed according to the manufacturer's documentation.

Some applications have certain restrictions, such as controlled access by requiring a password. Other applications are limited to the number of simultaneous connections they support. Each restricted application should have its own service.

Application services that are file services are assigned drive letters Q through Z. Disk services use the last two drives available for virtual disks. The designation of the last two drives available for virtual disks depends on the hardware configuration.

• Managing Printers

With MS-Windows or MS-DOS, the user can print files on a local printer (a printer connected directly to the back of the PC workstation) or a remote printer (a printer connected to a server on the PCSA network). This section describes the overall printing process and the various types of printing functions available.

Printing Process

Before discussing local and remote printing, it is helpful to understand the process of printing from MS-Windows, MS-DOS, or an application. An overview of the printing process is illustrated in Figure 3-2.

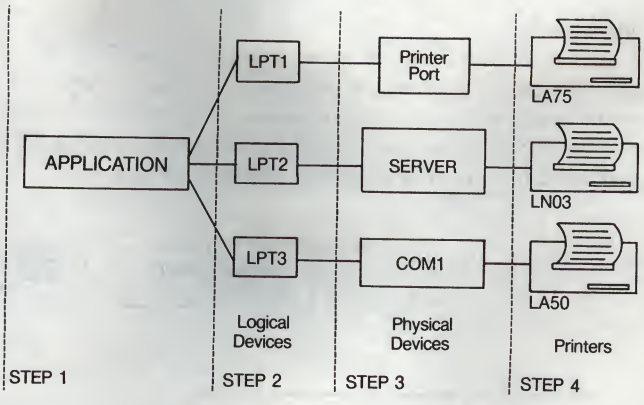


Figure 3-2 ▪ Overview of Printing Process

Step 1. The printing process starts when MS-Windows, MS-DOS, or an application is told to print a file.

Step 2. MS-Windows, MS-DOS, or the application sends the data to a logical device, which channels the data to the correct physical device. There are three logical devices—LPT1, LPT2, and LPT3—that can be associated with the physical devices.

Step 3. The logical device channels the data to a physical device, which is either a local printer port on the back of the PC workstation or a remote printer connected to a server on the network. By default, the PC workstation directs LPT1 to the local printer ports. These can be redirected to other physical devices.

The local printer port characteristics, such as baud rate, must match the local printer characteristics.

Step 4. The physical device, which connects directly to the printer, sends the data to the printer and the file prints. The system administrator maintains the list of local and remote printers available to the user.

Local Printing

Serial and parallel ports can be used for local PC workstation printing. Most PCs include one parallel and one serial port. Expansion cards with additional parallel and serial ports also are available from your local PC dealer.

Remote Printing

PCSA services allow the user to access remote printers. The user can use printers connected to a server as if they were local printers. Figure 3-3 shows a simplified configuration of a PC workstation and printers in a network. The figure shows a PC workstation connected directly to a local LA75 serial printer and connected by a server to a remote LN03 serial printer.

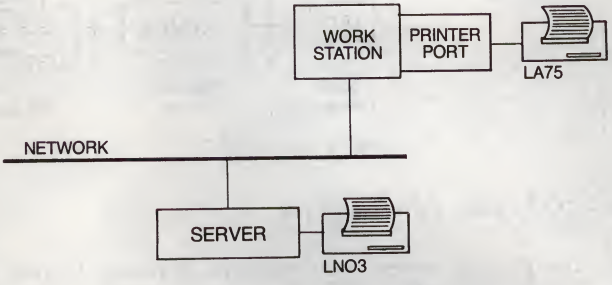


Figure 3-3 ▪ PC Workstation Using Local and Remote Printers

Logical Devices

Logical devices are pointers that channel data from an application to local printer ports and printers or to remote printers. There are three logical devices: LPT1 (or PRN), LPT2, and LPT3. By default, the PC workstation software assigns LPT1 to a local port. When a file is to be printed from either MS-DOS or MS-Windows, it is sent to the logical device, which directs the data to the correct printer.

Adding a Printer Service

A printer service allows PC workstations to connect to a directory to which they can spool print files. This option adds a printer service to the file server's service database and grants users access to the service. This is only necessary if the physical and generic queues and any necessary forms are set up for the printer. This task is performed using the PCSA_ADMIN File Server Options in order to:

1. Create the directory for the printer service.
2. Add the service to the file server's service database.
3. Grant all users read, write, and create access to the service.

Printers and Printer Drivers

The system administrator can add printer and printer driver files using the control panel installation menu. In addition, MS-Windows includes printer driver files for these unsupported printers:

- Enhanced drivers
  - IBM Graphics
  - LA75 Standard
  - LN03 Standard
- New drivers
  - LA210 DEC
  - LA210 Standard
  - LA210 Graphics
  - PostScript

Printing Modes

Some printers have more than one printing mode (such as the LA75 Companion printer). The LA75 has three possible printing modes to accommodate various hardware requirements:

- DEC mode

  The printer has full use of the Digital printer driver files and printer function.
- STD mode

  A Digital printer emulates an IBM Proprinter.
- HP mode

  A Digital serial printer emulates a Hewlett-Packard Ink Jet printer.

The system administrator can specify the mode in which the printer should operate when configuring the PC workstation.

▪ Printing from Applications

This section includes information about printing applications from MS-Windows and MS-DOS.

Using Printing Commands

Many applications have their own print commands. Whenever possible, use the application print command to send application files to a printer. For applications without print commands, both the MS-Windows Print command and the MS-DOS PRINT command are available.

Using LPT1

Some applications always direct data to be printed to LPT1. When using an application that always prints to LPT1, you must redirect LPT1 to the printer you want to use before running the application. For more information on redirecting logical devices, refer to the MS-DOS MODE command in the *MS-DOS User's Manual.*

Selecting Printer Types

The user specifies the printer type from the application. If a user was working with an application that did not recognize an LA75 Companion, but did recognize an IBM Proprinter, the system administrator has the option of setting up the LA75 to run in STD mode (IBM Proprinter emulation). To print from that application, the user tells the application that the printer is an IBM Proprinter.

Printing Screens

From MS-Windows and MS-DOS, users can press the Shift/PrintSc keys to print a currently displayed screen. Shift/PrintSc always directs that data to LPT1.

From the MS-DOS prompt, users also can print to the local printer on LPT1 using line echo. This will print what is displayed on the screen character by character. Not all applications support line echo. For these applications, nothing prints after the user presses CTRL/P. When control is returned to MS-Windows or MS-DOS, line echo resumes.

Selecting Default Printers

Some applications let the user select a default printer from within the application. The user can use the control panel (an MS-Window application) in the application to select a printer from the list of available printers.

End-of-File Markers

Some applications do not include an end-of-file marker when they send a file to the printer. An end-of-file marker is required when sending a file to a remote printer. From the application, the user presses the following keys

```
CTRL + ALT + PrintSc
```

to send an End-of-File marker.

Chapter 4 • PC Network Planning and Performance

Designing a network for optimum performance requires thorough planning. First the system planner must know the number of users, their applications needs, and how they are distributed physically. Once the network is running, the system administrator can then fine tune overall network performance using various system and client parameters. This section gives performance data based on the ideal configurations as well as suggested methods of fine tuning the network for optimum performance. This chapter is aimed at system planners and administrators, so the following suggestions assume familiarity with the Digital network utilities and VAX/VMS commands.

• Planning

To determine the distribution of users and applications on the network, the system planner must know the number of active users and where they are located. Active users are the number of users who actively use services at a given time; for example, the number of users accessing a database on the server, how often, and for how long. If many of the users frequently access databases, the users or applications should be distributed over a number of different servers to provide efficient system performance.

The physical location of users and their PC workstations can influence how the system planner distributes the users and applications to balance the server load. For example, if a group of users is doing a large amount of text processing and printing and their PC workstations are grouped together, it is logical to connect them to a nearby MicroVAX server with a printer. By physically grouping PC workstations, users, and the server together, you can minimize the amount of cable you need to install. However, if your system has users at a remote site, they must connect to the PCSA network using asynchronous communications. For further information regarding asynchronous communications, refer to *Chapter 2* and *Chapter 9* in this handbook.

Planning Considerations—Software

Users' tool and application preferences can affect how the network is managed. The system administrator needs to know the tasks and tools the users prefer, such as:

- Terminal emulation
- MS-Windows

- Word processing
- Spreadsheets
- Databases
- Printers and other sharable resources

In the personal computing environment, users traditionally could select and use their own applications. Unless a corporate standard has been established, often users in different departments use different applications for the same task. Consequently, when creating a network, it is difficult for planners to accommodate these different software packages. For example, different spreadsheet software packages create files that are formatted differently. For users to share data and maintain spreadsheets, these incompatibilities in data and output file formats must be resolved.

One solution is to standardize software tools. This solution is most effective if all end-user software tools are standardized across the company as part of a corporate data strategy. In this way, all users work with the same application packages and can share files without any difficulty.

Another solution to the problem of incompatible file formats is to provide a software program that translates incompatible files to a single, standard file format. In this way, users can keep using the tools they prefer and still share files they create.

Either one of these approaches solves the problem of diverse applications. The best solution depends on the particular office environment. In either case, file compatibility is a potential problem and should be addressed in the early planning stages.

Planning Considerations—Hardware

When planning out a network the system planner must ensure that PCSA supports the desired configuration. The system planner should:

- Determine what types of workstations, printers, and MS-DOS applications are expected to be configured.
- Ensure that the items to be configured are supported by referring to the SPDs.
- Resolve conflicts concerning unsupported hardware and software. It may be necessary to involve the sales representative or the delivery manager when resolving these conflicts.
- Determine the current system configuration.
- Prepare adequately by studying the documentation specific to the system configuration.

- Ensure that the hardware is operational.
- Determine on what type of processor the server software will be installed.
- Decide whether or not the server software will be installed on a VAXcluster system.
- Determine what types of processors are members of the VAXcluster system.
- Decide what types of PC workstations will be configured into the network.
- Determine what type of Ethernet board will be used.

These guidelines are used in the *DECstart Delivery Guide* (for more information about the DECstart Program, refer to *Chapter 11*). By compiling this information at the outset, your system planner will be better prepared to work with a Digital representative to determine your specific configuration needs.

▪ PCSA Performance Data

Digital conducted performance testing to determine how many active PC clients can be supported.

Three different MicroVAX configurations were tested:

- MicroVAX 2000 with RD54 disks
- MicroVAX II with two RD53 disks
- MicroVAX II with RA81 disk

The number of PCs varied for each test, ranging from 1 to 50 simultaneously active clients for the MicroVAX II configurations, and 1 to 40 simultaneously active clients for the MicroVAX 2000 system.

The workload assumed "typical" office activities and applications: word processing, spreadsheet, database management, and terminal emulation.

The PCSA server test was a hybrid mix of disk services and file services. This mix takes advantage of the benefits of both services: the file-sharing capabilities of the file service and the high-speed access capabilities of the disk service for read-only MS-DOS files. MS-DOS applications resided on a read-only disk service. Spreadsheet and word processing files were stored on a read/write file service—one service for every PC client.

Figure 4-1 shows the overall performance profile for the three configurations. The server response time was compared to writing to/from a local hard disk drive on a standalone IBM Personal Computer AT. Where the ratio was greater than 1, the PCSA server took longer to execute the reads and writes than the standalone hard disk. Where the ratio was less than 1, the response time of the PCSA server was better than that of the standalone system.

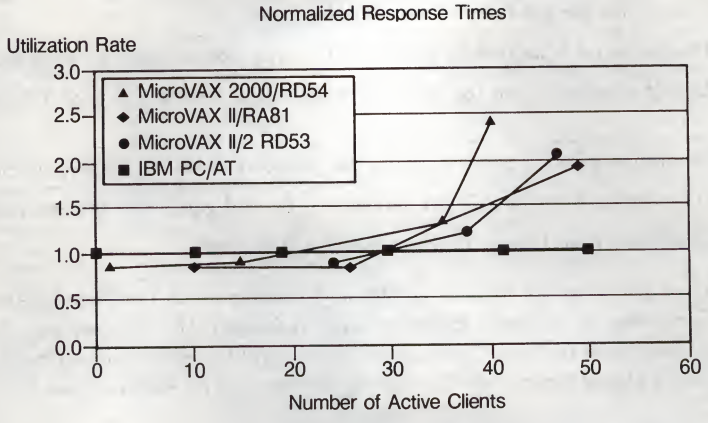


Figure 4-1 ▪ VAX/VMS Services Version 2.0 Performance

A MicroVAX 2000 with one RD54 disk can support 21 simultaneously active floppy-only client PCs running the sample application mix with performance comparable to the speed of a standalone IBM Personal Computer AT hard disk. For less than 21 simultaneously active client PCs, the performance is better than the IBM Personal Computer hard disk. When the number of clients is increased to 40, the performance is comparable to about 50 percent of hard disk performance.

This testing was performed on a MicroVAX 2000 with 3Mb of memory and a disk services cache size limited to 512 pages. Increasing the cache size to 1024 pages with a standard 4Mb MicroVAX 2000 significantly increases the performance.

A MicroVAX II can support 30 simultaneously active floppy-only client PCs running the sample application mix with a performance of a standalone IBM Personal Computer AT hard disk.

Competitive Comparisons

In competitive situations, the duty cycle—the fraction of the time that PCs are active—often becomes an important factor. PC LAN vendors quote numbers of subscribers or connections on a server against simultaneous use numbers. "Simultaneous use" means using the server, not PCs being used simultaneously without server participation. Many vendors can only support a few simultaneously active users with acceptable performance.

▪ Performance Tuning

PCSA provides a number of options as follows for fine tuning the network:

- SYSGEN parameters
- Network parameters
- File server parameters
- Virtual disk service
- PC tuning
- Third-party Ethernet card tuning
- General tuning

SYSGEN Parameter Tuning

SYSGEN is a system generation utility. The SYSGEN parameters are modified to tailor an operating system for a particular hardware configuration with modifications and additions to the software configurations. It is a utility that can be used to manipulate the cache hit ratio for both the disk and file servers.

- *Disk Server*

  The SYSGEN parameters that affect the disk server are modified at the VAX/VMS level. The cache hit ratio is checked. If it is not high enough, it is increased. If more memory is needed, the memory usage and page rate is checked. The SYSGEN parameters NPAGEVIR (nonpaged virtual pool) and NPAGEDYN (nonpaged pool) are used to increase the disk server's cache size.

- *File Server*

  The SYSGEN parameters that affect the file server also are modified at the VAX/VMS level. The MONITOR FILE is first checked to find out what the average hit ratio is on the directory data and file headers. If the hit ratios are too low, the SYSGEN parameters ACP_DIRCACHE and ACP_HDRCACHE are used to increase the number of directory and header blocks that are cached.

  The WSMAX parameter also can be modified so the file server can use a larger working set size.

Network Parameters

The Network Control Program (NCP) is a DECnet management utility. The NCP parameters, along with the type of nodes (routing versus nonrouting) you use, affect the overall network performance.

NCP can be used to adjust any of the following parameters:

- Incoming/outgoing timers
- Delay factor
- Delay weight
- Retransmit factor
- Pipeline quota

Routing nodes can have a buffer size of 576 bytes, and end nodes can have a segment size of up to 1400 bytes on the Ethernet. Nonrouting nodes do not have the overhead of processing routing updates.

For more detailed information about NCP, refer to *Chapter 9.*

File Server Parameters

Further file server tuning can be done through VAX/VMS. Use the SHOW SYSTEM command and note the page fault rate on PCFS_SERVER process. If the page fault rate is 800 to 900, no action is required. If the page fault rate is higher than 900, the page fault rate must be decreased. The MAXIMUM_WORK_SET must be increased in the PCFS_STARTUP.COM file (the command file that initiates PCSA software).

Virtual Disk Service

To ensure optimal performance, the multicast traffic on the LAN should be kept to a minimum. Also, the /R:switch should be specified when the virtual disk software is started with the NET START LAD command.

PC Tuning

Memory can be saved on the PC workstation by considering the following:

- Save memory by not using the DEPCA card in reduced buffer mode.
- Use MS-NET if all functions of NETBIOS are not required.
- Load only the drives that are used.
- Minimize buffer space.
- Use both file and disk servers.
- Use terminal services (LAT).

Third-Party Ethernet Card Tuning

On an IBM Personal Computer XT, the following commands are used to disable multicast address filtering:

- NET START LAT /M:DISABLE
- NET START LAD /M:DISABLE /R:1 /W:1
- NET START RDR /M:DISABLE
- NCP SET LINE MULTICAST DISABLED

NET and NCP are DECnet utilities executed at the MS-DOS command line.

The following NCP parameter values can be changed on the IBM Personal Computers XT and AT, and on IBM compatibles:

- Incoming timer
- Outgoing timer
- Delay factor
- Delay weight
- Retransmit factor
- Maximum buffers
- Transmit pipe quota
- Receive pipe quota

General Tuning

For ovetall system tuning, consider the following:

- Set the Asynchronous System Trap (AST) limit for the file server process to twice the number of PCs actually supported.
- Set the VAX/VMS executor PIPELINE QUOTA greater than 6000. The RECEIVE PIPE QUOTA should not exceed 1 and should be greater than the NAK QUOTA.
- Use a LAD driver instead of a file server for system software if there is only one user writing data or multiple users reading data.
- Take slow devices out of the path list.
- Distribute user services among available systems and distribute services among disk controllers.

Chapter 5 · Security for PC Files

Many companies deal with sensitive information such as personnel files, corporate financial data, corporate strategies, and product specifications. When this data is stored on a computer, data security is crucial. For many system planners and administrators, the ability to secure data is a major factor in determining which server to use and how to configure the PCs in a network.

VAX/VMS Services for MS-DOS gives you the full range of VAX/VMS protection to secure the PC files and directories stored on VAX/VMS disks, printer services, and in VAX/VMS directories. For instance, if a MicroVAX server is dedicated to a department, the system administrator can limit unauthorized access to the data stored on the server. Additional security is gained if the server and clients connected to it are made into a departmental network, separate from and inaccessible to a larger network.

Some of the key security features of VAX/VMS Services for MS-DOS are:

- Separate listing of user profile information
- Listing of current connections, file opens, sessions, and available services
- VAX/VMS Access Control Lists (ACLs) support
- Cluster-wide locking support

· VAX/VMS Security Features

VAX/VMS affords a high degree of security. It provides mechanisms for controlling access, securing the database, and creating an audit trail. Among the security features of VAX/VMS are the following:

- A user entry and password system
- An operations log that includes provisions for alerting security staff of ongoing security breaches
- An encryption system that provides a higher level of security for sensitive files

VAX/VMS runs on all VAX hardware and is compatible with the MicroVAX, thereby facilitating both upward migration and networking. This operating system was evaluated by the National Computer Security Center and in August, 1986, was rated at the C2 level. VAX/VMS is the first minicomputer general operating system to receive a C2-level security rating.

One advantage of VAX/VMS is the flexibility in implementing its security features. For example, file protection features can be invoked to protect all, some, or none of your files. Similarly, you can make provisions for the use of passwords, locked passwords, or no passwords. The use log may be ignored, used only for record keeping, or employed as a security tool.

By selectively using the various security features of VAX/VMS, you can provide a high degree of security for sensitive data while dispensing with or reducing control procedures for less critical information. After analyzing your specific security needs, you can use the security capabilities of VAX/VMS to control access, discourage random abuse, and deter serious compromise. In short, VAX/VMS provides all the control that can be expected reasonably of a general-purpose operating system, while inconveniencing legitimate users in only minor ways.

Access Control Features

The essence of system security lies in controlling access to data. An authorized user, by definition, is entitled to access at least some data on the system. This access may be limited severely. For example, a user may be authorized to access only one file on the system and may have read-only access. Another user may be authorized to change the contents of the file, as well as read it. A third user may be authorized to read the file, change its contents, and delete it. These three individuals are all authorized users, but the nature of their authorized use is defined sharply and varies from one to another. A fourth user may not be authorized to access the system at all and would be considered an intruder.

The primary control mechanisms VAX/VMS uses to restrict access are ACLs and User Identification Codes (UICs). The ACL uses identifiers to specify users. The three types of identifiers are:

- UIC identifiers, referring to each user on the system
- General identifiers, specified by the security manager to refer to groups of users
- System-defined identifiers, describing users based on their use of the system

System-defined identifiers are defined automatically by the operating system when access rights are created at the time of system installation. They are categorized as BATCH, NETWORK, INTERACTIVE, LOCAL, DIALUP, and REMOTE.

A user is assigned automatically one of these identifiers during login, and the VAX/VMS login software adds the appropriate identifier to the process rights list. In addition, an ACL may be constructed to restrict access to a dataset to particular individuals or categories of users.

An ACL consists of one or more Access Control Entries (ACEs). The three security-related ACEs are:

- An identifier ACE, which controls the type of access permitted to an individual or group. Access types are READ, WRITE, EXECUTE, DELETE, CONTROL, and NONE.
- A default protection ACE, which defines the default protection for directory files only.
- A security alarm ACE, which provides an alarm message to alert managers to possible security breaches when designated forms of access (READ, WRITE, EXECUTE, DELETE, or CONTROL) are accomplished or attempted.

User Identification Codes

Each system has a UIC, while each system object also has an associated UIC, defined as its owners' UIC. Each system UIC also has a protection code relating a user with permitted types of access.

Thus access to objects is controlled by the relationship between the UIC of the user and the UIC of the object.

All users seeking access to the system fall into one or more of the following categories within the system:

- System, which includes all users who have system privileges
- Owner, which means the user who created the object to be accessed and therefore has the same UIC
- Group, which includes all users with the same group number in their UICs as the object's owner
- World, which includes all users

The protection code uses these categories to permit or deny READ, WRITE, EXECUTE, or DELETE access.

When a user logs in, the identifiers that are in the user's rights database are copied into a rights list that becomes part of that person's process. (The process includes the user's UIC and the system-defined identifiers.) VAX/VMS uses the rights list to perform all protection checks.

While logging in is a simple procedure from the authorized user's point of view, from the system's point of view it is not simple to grant or deny access.

Login sets in motion a sophisticated and highly complex process that determines the kind of access (if any) permitted to the user, what objects the user can access, and what the user can and cannot do with those objects.

Logging In

Users gain access to the system by logging in. Login is an initial screening process that permits the system to clear a user who is attempting access. The login process usually requires both a username and a password so the system can check authorization and impose restrictions. Different classes of login accommodate all possible modes of access. Logins fall into two categories: interactive and noninteractive.

An interactive login is accomplished when the user follows system prompts that appear on the terminal screen. For example, a local login might involve specifying the system on which you have an account when prompted to "SELECT SYSTEM," typing your name at the "Username:" prompt, and typing your password at the "Password:" prompt. In this case, you are providing information requested by the system, and the system is responding to your input. To access the system, you must input all three items of information correctly. In other words, you must specify a system that can be accessed on the terminal you are using, the username must be authorized to access that system, and the password must match that of the username. Analogously, you open a combination lock by dialing the required digits in the proper order.

A noninteractive login is performed by the system without user/system interaction.

Types of interactive logins are local, dialup, and remote.

Local logins are executed by a user who is directly connected to the system.

A dialup login requires the same procedure as a local login. In this case, the terminal/system connection is accomplished by using a modem.

Remote logins involve the same procedure as a local login, the difference being that remote logins are performed to a node over a network.

Type of noninteractive logins are network, batch, and subprocess.

A network login involves a user accessing a file stored in a directory on another node or performing a network task on a remote node, assuming that both nodes are on the same network.

A batch login is a noninteractive login procedure accomplished when a batch process initiated by a user starts to run.

A subprocess login is another noninteractive login that results from a user executing either a specific process form of a command or a system service.

Passwords

Passwords are used as part of the login process. In many environments, a user password suffices to access the system. As an added security precaution, a system password may be required before the user password. In maximum security environments, two user passwords, entered successively, may be required for access.

Passwords may be selected either by the user or generated automatically. Passwords may consist of letters, numerals, or a combination of both. Security is enhanced by requiring a minimum character length for user-generated passwords and by creating pseudowords resembling English in the automatic generation mode. In addition, VAX/VMS can limit the number of password entry attempts in order to discourage attempts to guess a password.

All passwords are stored in a one-way encrypted form. One-way encryption ensures that no individual, including the system manager, can determine an actual user password.

If a user forgets his/her password, the system manager can assign a temporary password to allow the user to log in to his/her account: then the user should select a different password. The system manager can force the user to enter a new password by "expiring" the temporary password.

System Operation

VAX/VMS security features are based on the reference monitor concept, using the reference monitor as the central security point for subjects, objects, the reference monitor database, and security auditing.

When a user logs in, VAX/VMS creates a process with the user's identity. The process gains access to information as the user's agent in the system. Process creation and access to information by processes are critical mechanisms by which the operating system enforces security. Because process creation raises a number of potential security problems, many security features of VAX/VMS focus on this area. A user attempting to log in must provide both a username (which is given to the resulting process) and a password. The file of encrypted user passwords becomes part of the reference monitor's database. VAX/VMS provides additional password security by storing encrypted passwords in a file that is normally excluded from general access.

After a process is created, VAX/VMS assigns it a UIC, which corresponds to the UIC of the user creating the process. The UIC also indicates the group to which the user belongs. Other information may be attached to the process—for example, the affiliation of the process's owner with various other groups. The most basic objects in the reference monitor concept are files and directories. These are protected in a number of ways from unauthorized access, whereas a variety of mechanisms allow controlled sharing of data.

Objects other than files and directories can be used to store sensitive data. Among these objects are sections, mailboxes, logical names, and event flag clusters.

In the reference monitor concept, each subject's authorization to gain access to an object is contained in the authorization database. The database is distributed and stored in association with objects that must be protected. For example, the authorization data for a directory is included in the header for that directory.

VAX/VMS permits great flexibility in the implementation of its security features. Most objects are protected on a UIC basis, which specifies whether access is allowed or denied to processes acting on behalf of system management, the object owner, other members of the same UIC group as the owner, and all other users.

In addition to UIC-based protection, files and directories can be shared under control of ACLs that list users or groups allowed or denied access to particular files and directories. ACLs specify sharing on the basis of UIC and other identifiers associated with a process.

For example, it is possible to specify that a file not be read by a process connected to a dialup line, thereby preventing unauthorized access from a remote location.

Auditing Features

Detection of possible security breaches is an important element in system security. VAX/VMS allows a terminal to be designated as an audit alarm console on which all auditable events may be displayed. Such events may include login failures and successful or unsuccessful attempts to access sensitive files. Events may be audited at the discretion of users and security managers. For example, the owner of a particular file can create an ACL entry requesting that any attempt to access that file be audited.

DECnet Security

As might be expected, there are similarities in the basic reference monitor concept—whether the system to be protected is a single system or a network.

The implementation of the reference monitor concept is more complex because in accessing an object across a network, one must think in terms of two systems: one containing the subject seeking access; and one, the object.

Since each computer's reference monitors can deal only with subjects and objects on their individual systems, an access attempt across a network will involve a phantom object and a real subject on one system, and a phantom subject and a real object on the other.

Of the various means VAX/VMS provides to establish correspondence between a subject or process on a source node and another on a target node, use of proxy accounts offers distinct advantages. The target reference monitor must maintain a table of source subjects (specified by user name and node name) and the corresponding target (or local) user names. Each request from a subject on a source node then is mapped into the creation of a subject representing the corresponding target user. This mechanism offers the explicit control associated with username/password control while adequately protecting passwords.

Network operations security depends on the ability of source and target reference monitor mechanisms to communicate in a private and authentic manner. Obviously, it is critical that an intruder be unable to observe passwords or mimic a source node that has been granted proxy access. The most effective methods of achieving such protection are physical protection, such as that afforded by conduits and encryption. The Digital Ethernet Security Network Controller (DESNC) and the VAX Key Distribution Center software package (VAX/KDC) are designed to enhance Ethernet security.

DESNC controllers for Ethernet LANs upgrade security through data encryption. DESNC controllers provide transparent cryptographic security at a level consistent with the National Bureau of Standards Data Encryption Standard. Specifically, the DESNC controller is a store and forward device that provides real-time cryptographic process of Ethernet frames (messages) over an Ethernet LAN. Decryption restores the data to its original form through a client node that takes advantage of encryption/decryption services.

A DESNC controller can accommodate any combination of workstations, servers, or VAX processors. Operating system software that can run on client nodes supported by the DESNC controller includes VAX/VMS, RSX, and ULTRIX. VAX/KDC is a VAX/VMS layered product that serves as the central authority for managing the DESNC controllers and enforcing security policy for an Ethernet LAN or extended LAN. Multiple VAX/KDC nodes may be used to improve the availability of the networked DESNC controllers.

▪ File Server Security

The file server provides two levels of security:

- Access to services granted by the system administrator
- Access to files using VAX/VMS file protection read/write features (including VAX/VMS Access Control Lists), which provide the user with the convenience of a LAN coupled with the sophisticated security of VAX/VMS

This two-level security access allows PC workstations to connect to the same service with differing access rights.

Service Access

The system administrator can grant service access to an individual user or to all users. For each user, the file server maintains a list of services to which the user can connect. The file server also maintains a list of services to which all users can connect. The file server maintains these lists with the service database. When a client connects to a service, the file server checks the service database and grants the user the appropriate access. The system administrator can grant privileges using the PCSA_ADMIN utility or the PCSA GRANT command, when services are added.

For example, to grant users alias SMITH and JONES access to the service VXSYS using the PCSA GRANT command, a system administrator executes the following steps at a DCL prompt:

```
$ PCSA GRANT SMITH VXSYS /ACCESS=READ

$ PCSA GRANT JONES VXSYS /ACCESS=(WRITE,READ)
```

Both users can connect to the VXSYS service, but SMITH has read access and JONES has read/write access.

File Access

The file server determines a user's access to a file according to two criteria:

- The type of service to which the user is connecting (system, application, common, or personal)
- The VAX/VMS account used when connecting to the service

If the service is listed in the service database, the file server also determines the type of access that the user is granted to the service. The file server uses these criteria to determine the user's access to files in the service.

If the user connects to a system or application service listed in the service database, the file server looks at the type of access granted to the user to determine file access privileges.

If the user connects to a personal account listed in the UAF or a common service, the file server checks the user's UIC, privileges, and identifiers to determine if VAX/VMS allows the type of access requested. This checking is the same type VAX/VMS performs if the user attempts access while logged in at a terminal.

If the user does not have an account, the system administrator can use the PCSA_ADMIN utility to create a new one.

When a client does not specify a VAX/VMS account in the NET USE command, the file server only allows connections to services with public access.

Because of the multilevel security, a client must have write access to both a file and a service to write to a file. If a user has read access to the service MONTH and has write access to the file REPORT.TXT, the user can only read the file. If a user has write access to the service MONTH and has read access to the file REPORT.TXT, the user can still only read the file.

A user can connect to an account listed on the UAF if the user knows the password for the account. For example, to access the account JONES, user JONES types:

```
NET USE H:\\node\JONES [password]
```

User JONES has full access to the default directory specified in the UAF for JONES.

For user SMITH to access the service also, he/she types:

```
NET USE H:\\node\JONES%SMITH [password]
```

In the second example, JONES represents the service name JONES, which is a UAF entry. But user SMITH has access granted to JONES according to the account SMITH. In VAX/VMS, this procedure is equivalent to setting the default directory to another user's directory.

▪ Virtual Disk Security

The system administrator is responsible for protecting each virtual disk with a password. A virtual disk can be mounted so that the disk server associates a password with the virtual disk service. The disk server stores the password in the disk server's service database. When the VAX computer is rebooted, the disk server remounts the virtual disk with the same password. Once a password is assigned to a virtual disk, a user must specify the password to gain access to that disk.

The command PCSA SET DISK_SERVER SERVICE PASSWORD allows the system administrator to change the password of a mounted virtual disk.

Chapter 6 • Third-Party PC DOS Applications

Digital has tested the top-selling PC applications designed and licensed for network use, including those from Lotus Development Corporation, ASHTON-TATE, and WordPerfect. All of these applications are supported by the PCLAN/Server 2000 and in larger PCSA environments.

It is the system administrator's responsibility to ensure that users comply with the terms and conditions of each software license agreement entered into when an application is installed on the VAX/VMS server. Each license defines the number of users and/or simultaneous users for an application. The system administrator must set the number of users of an application to match the number of users covered by the software license. Exceeding the number of users for which you are licensed violates your license agreement.

Some third-party applications are not designed to run on a network. The third-party vendor can answer your questions regarding networking provisions and licensing.

The PCSA software was designed to accommodate existing office environments. Consequently, the ability to add third-party applications was built into the PCSA software. This section explains how to add an application through the PCSA_ADMIN utility.

• Adding an Application Service on the File Server

The PCSA_ADMIN utility maintains the file server options including adding and deleting system, common, application, personal, and printer services, as well as listing directory and file services.

The system administrator must add an application service for each MS-DOS application installed on the file server. The system administrator uses the PCSA_ADMIN utility to add a new application service. The utility will prompt you for the following information:

- The application service name (for example, MSWORD).
- The alias for the service. The alias is another name assigned to the same service. Users specify the alias when connecting to the service. The default name for the alias is the service name.
- The directory specification for the service. The PCSA_ADMIN creates a default directory PCFS$APPLICATION:[Service_name] if one is not specified (for example, PCFS$APPLICATION:[MSWORD]).

- The user to whom you want to grant read, write, and create access to the service. This user is usually a system administrator or another individual who has system privileges. As a default, PCSA_ADMIN grants read, write, and create access to the SYSTEM account.

As the PCSA_ADMIN utility runs through the procedure for creating an application service, it verifies the tasks on screen as they are completed. After this procedure is run successfully, the application service is accessible from a PC workstation. The third-party application then can be installed according to the manufacturer's documentation.

• Installing an Application on a Disk Server

To install an application on a disk server the application must reside on a virtual disk. The application then is offered to the network through the disk server. The virtual disk first is created and then mounted for use throughout the network.

To create and format an MS-DOS virtual disk file, use the PCSA Manager utility (PCSA_MANAGER). The PCSA_MANAGER utility will not create a virtual disk file if a file by the same name already exists in the target directory. For example, to create and format a 5Mb virtual disk for the application MULTIPLAN and allocate 5000 blocks to the disk, at the PCSA_MANAGER prompt the system administrator types:

```
PCSA_MANAGER>CREATE DISK MULTIPLAN /SIZE=5MB /TYPE=APPLICATION
/ALLOCATION=5000
```

Confirmation messages then appear on the screen.

The /TYPE=APPLICATION qualifier tells the PCSA software to create an application virtual disk.

A virtual disk file has been created called MULTIPLAN.DSK. The next step is to mount it. To install an application on the virtual disk, it must be mounted with write access. For example, to mount the virtual disk file MULTIPLAN.DSK permanently on all nodes in the cluster, the system administrator uses the PCSA_MANAGER utility and types:

```
PCSA_MANAGER>MOUNT DISK MULTIPLAN/TYPE=APPLICATION/CLUSTER/PERMANENT
```

Confirmation messages then appear on the screen.

The /PERMANENT qualifier means that the disk server automatically remounts the virtual disk upon startup.

At this point, the virtual disk is mounted and the application can be installed. Once the application is installed successfully, dismount the disk and then remount it with read-only access. To dismount the virtual disk, the system administrator, at the PCSA_MANAGER prompt, types:

```
PCSA_MANAGER>DISMOUNT DISK MULTIPLAN
```

A confirmation appears on the screen.

Once this is completed, remount the disk with read-only access.

A quick review follows, showing the steps to install an application on a disk server.

1. Create the application virtual disk.
2. Mount the application virtual disk with read-only access.
3. Access the drive using the NET USE command from the client.
4. Install the application according to the manufacturer's documentation and licensing agreements.
5. Dismount the virtual disk.
6. Remount the virtual disk with read-only access.
7. Store the resulting data files on a file service.

Chapter 7 · Programming in the PCSA Environment

The relationship between the various network components is governed by a set of standards called the Digital Network Architecture (DNA). The DNA is the network architectural model upon which Digital's communications products are based. This chapter discusses the basic structure of the DNA, the PCSA software interfaces, and DECnet-DOS programming concepts.

· Digital Network Architecture

Digital's networking capabilities are based on the DNA. Since 1975, Digital has adhered to DNA, which serves as the blueprint for virtually all past, present, and future communications products. Historically, the DNA model, like the Open Systems Interconnection (OSI) reference model, is arranged in independent layers. Each layer can be changed without significantly affecting other layers. In each layer, the protocols govern communication with other layers.

As DNA progresses to its next phase, it will comply with the OSI reference model depicted in Figure 7-1.

Digital's implementation of DNA is DECnet. DECnet software is layered on each of Digital's operating systems, allowing all Digital systems to communicate across the network with compatible functions.

DNA's layered structure has provided DECnet software with a unique adaptive quality. Since DECnet was first announced, it has progressed through four phases, each providing increased capability. Now Digital has announced the next progression, DECnet/OSI Phase V, which promises compliance with international standards by merging DECnet and OSI.

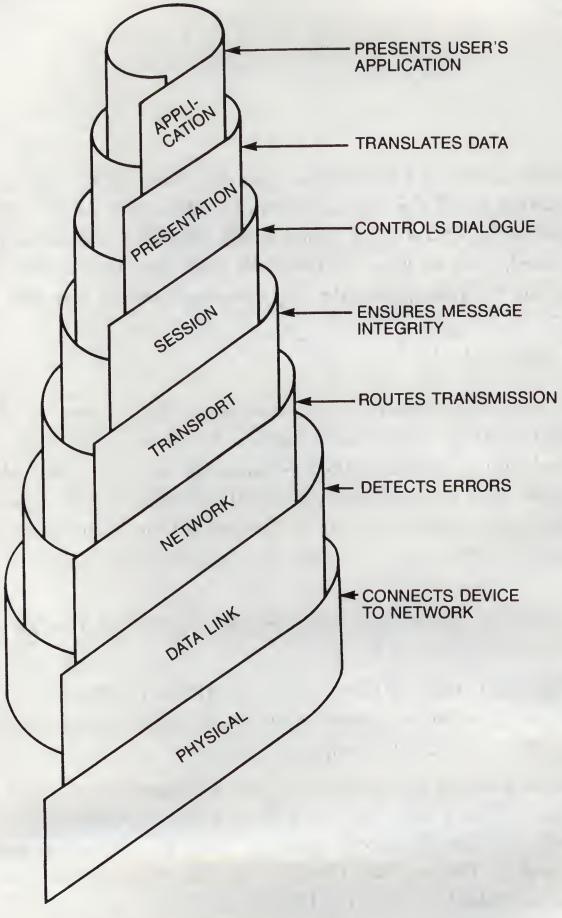


Figure 7-1 • Open Systems Interconnection Model

• Interfaces

Interfaces can be considered as boundaries between the different DECnet software components in a single node. These boundaries are arranged as hierarchical layers. The DECnet software is defined as modules within these layers, ranging from highest to lowest. Table 7-1 illustrates how the DNA layers correspond to the OSI layers.

Table 7-1 ▪ OSI and DNA Corresponding Layers

Open Systems Interconnect Model	Digital DNA
Application	User
Presentation	Network application
Session	Session control
Transport	End-to-end communications
Network	Routing
Data link	Data link
Physical	Physical link

DNA describes how each layer of software builds on the services offered by modules in the lower layers. DECnet is designed in this way to allow high-level network functions (such as task-to-task communications) to occur in an orderly and predictable way on each DECnet node. For these network functions to work properly, a set of rules or protocols must be followed. The protocols are very specific, allowing for effective communication among the different nodes in the network.

There are many advantages to using a layered architecture. They include the following:

- The same architecture can be run on all your systems, whether they are PDP-11 computers, VAX systems, or PCs.
- The application programs you create can run on any configuration, whether you are using Ethernet, serial line, or satellite connections.
- The programs you develop can run on future releases of network products, which will let you take advantage of new communications technologies.
- Software investments are protected, but you can still take advantage of latest network technologies.

▪ Session Interfaces

PCSA software provides standard and Digital proprietary interfaces underlying the network. In addition to direct access to the data link layer, there are network interfaces called session layers.

The interfaces for applications running in a network environment enable programmers to design applications that work transparently with the PCSA software. DECnet/PCSA Client software provides three interfaces to networks:

- DECnet socket library
- Microsoft Networks (MS-NET) session interface
- NETBIOS session interface

DECnet-DOS software provides the DECnet socket interface. The system administrator must select the network interface for each PC workstation using either the MS-NET or NETBIOS interface.

MS-NET is a communications protocol developed by Microsoft. The MS-NET session interface is a subset of the NETBIOS interface. MS-NET is provided to save memory if all of the features of NETBIOS are not required. With MS-NET, you can run the redirector, which is the MS-DOS software that sends calls for MS-DOS drives to a remote server. However, MS-NET does not include support for NETBIOS adapter names or NETBIOS datagrams.

The NETBIOS interface is required to run some third-party MS-DOS applications. Most applications that allow file sharing on the file server use MS-DOS byte range locking. In that case, MS-NET can be used in place of NETBIOS. NETBIOS is necessary to provide support for adapter names and datagrams.

Table 7-2 shows the functions available in MS-NET V1.0, MS-NET V2.0, and NETBIOS V2.0.

Table 7-2 ▪ Session Differences

Function	V1.0 MS-NET	V2.0 MS-NET	V2.0 NETBIOS
Memory	22Kb	23Kb	27Kb
Transparent	Y	Y	Y
Naming service	N	N	Y
Datagrams	N	N	Y

Table 7-2 • Session Differences (Continued)

Function	V1.0 MS-NET	V2.0 MS-NET	V2.0 NETBIOS
Asynchronous DECnet	Y	Y	Y
INT 5C	N	Y	Y
INT 2A	Y	Y	Y
Extended	Y	Y	Y
Remote adapter	N	Y	Y

VAX/VMS Services for MS-DOS and DECnet-DOS support the NETBIOS programming interface. NETBIOS applications will run unmodified on PCs running DECnet-DOS and DECnet/PCSA Client software. NETBIOS applications then can communicate transparently over both LANs and WANs. The NETBIOS applications also can communicate with non-PC DECnet nodes such as VAX/VMS and ULTRIX.

• DECnet-DOS Utilities for Network Programming

Since DECnet/PCSA Client software is a superset of DECnet-DOS, all of the programming tools included in DECnet-DOS are included with the DECnet/PCSA Client software.

DECnet software offers programming interfaces that enable programmers to take advantage of the capabilities of DECnet and create distributed applications that suit specific needs. The DECnet software provides source files needed to create a programming library. These files include:

- C language sources
- Assembly language sources
- Header files that contain definitions for the network interface

• DECnet-DOS Programming Concepts

Using the C or assembly language programming interface, programmers can write PC-based network applications to access network resources and implement task-to-task communication for DECnet client and server tasks. The following mechanisms enable programmers to access those high-level network functions:

- Logical link
- Sockets
- Client and server tasks

A logical link is a temporary conversation between two communicating programs (or processes) in a DECnet network. DECnet implements logical links to facilitate the flow of information between two programs or processes. Logical links are created by the interaction of DECnet calls in the two cooperating programs. This interaction is referred to as the "handshake procedure." In this procedure, DECnet calls are passed between two programs to establish an agreement to communicate. A logical link is created when both programs agree.

Sockets are the basic building blocks for DECnet-DOS task-to-task communication. A socket is an addressable endpoint of communications within a program or task. A task uses the socket to send data to and from a similar socket in another task. Sockets contain information about the status of the logical link connection. Figure 7-2 shows basic building blocks for task-to-task communication.

DECnet-DOS supports two kinds of sockets: stream sockets and sequenced packet sockets. Stream sockets cause bytes to accumulate until internal DECnet buffers are full. The receiving task does not know how many bytes were sent in each write operation. Sequenced packet sockets cause bytes to be sent immediately. The receiving task receives those bytes in one record.

A DECnet-DOS program can detect any potential problems by polling the socket's status or by receiving error status in response to network requests.

Client and server tasks are programs that communicate through sockets. These tasks exchange data over logical links.

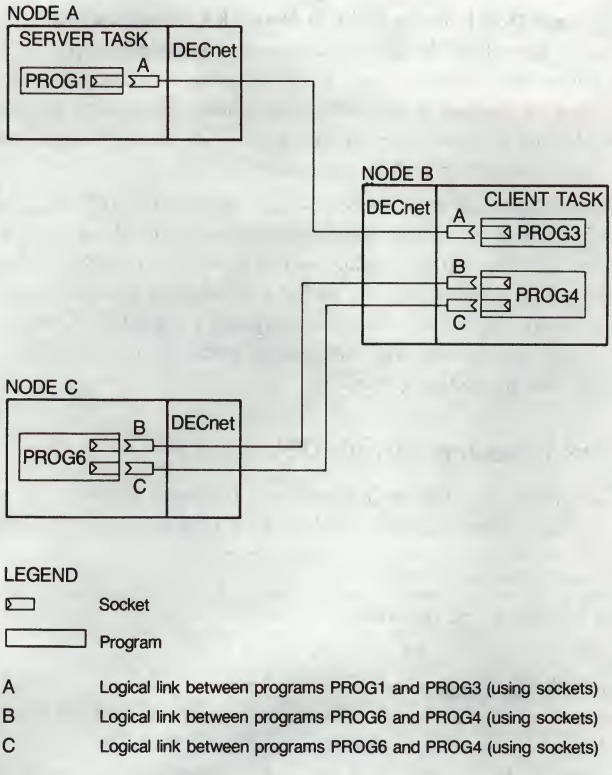


Figure 7-2 ▪ Sockets: Basic Building Blocks for DECnet-DOS Task-to-Task Communication

DECnet-DOS communication requires cooperation between two programs or tasks. For the purpose of defining the DECnet-DOS programming interface, there is a distinction between the client task, which initiates a connect request, and the server task, which waits for and then accepts or rejects the connection.

Once a logical link is established, the client and server tasks have a peer-to-peer relationship. The operations performed on their respective sockets are symmetrical. Either task can act as the source or receiving task and can send and receive data or terminate the logical link at any time.

Using DECnet-DOS Function Calls in Network Communications

To create a logical link, the server task creates a socket supported by DECnet. When this socket is first created, it has no assigned name or number. An object name or number is assigned to the socket. The name or number is required for use in future listening operations. The socket declares itself as a server that is available for client connections.

In turn, the client task must create a socket supported by DECnet. The client task can set up access control information and/or optional connect data. The system returns an integer value called a socket number. Subsequent DECnet-DOS function calls on the socket will reference this associated socket number. At this point, the client task requests a logical link connection to another task. Any optional user data and/or access control information is sent along with the connection request.

▪ Network Programming with DECnet-DOS

After you install the DECnet-DOS software and configure your DECnet-DOS node, you can perform a variety of high-level network functions, including:

- Task-to-task communication
- Remote file access and file transfer

Task-to-Task Communication

Task-to-task communication is a feature common to all DECnet implementations. It allows task or application programs to communicate with each other. Cooperating tasks on different nodes issue DECnet calls that enable them to exchange data over a logical link. Because all DECnet products are designed in accordance with DNA specifications, all DECnet implementations (and applications created with them) can communicate with each other.

DECnet-DOS supports two forms of task-to-task communication: transparent and nontransparent. Transparent communication provides a subset of functions that a program uses to exchange data with other programs. Nontransparent communication allows programmers to use the full range of DECnet-DOS task-to-task communications.

- *Transparent Communication*

DECnet-DOS supports transparent task-to-task communication for any high-level language and assembly language programs. Using specific calls, a task can perform standard I/O operations and communicate with another task over the network. This form of I/O lets you move data with little concern about the underlying DECnet interface.

User-written applications can use transparent task-to-task communication after the DECnet-DOS software component Transparent Task-to-Task (TTT) has been installed. This utility provides the basic functions necessary for tasks to communicate over the network, including:

- Initiation and establishment of a logical link
- Orderly exchange of messages between both tasks
- Controlled termination of the communication process

Figure 7-3 illustrates the sequence of events that occur during transparent task-to-task communication.

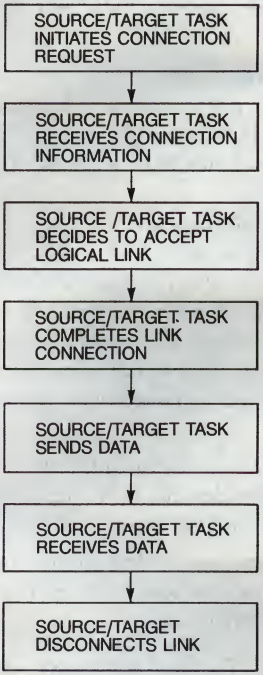


Figure 7-3 ▪ Transparent Task-to-Task Communication

You can use the DECnet-DOS Transparent Network Task Control Utility (TNT) to display information regarding a TTT session. The TNT utility returns standard MS-DOS error messages and extended error messages that help you locate problem areas.

- *Nontransparent Communication*

  DECnet-DOS nontransparent communication provides the same functions as DECnet-DOS transparent communication but with additional system and I/O functions. For example, you can use network protocol features such as optional user data on connects and disconnects and out-of-band messages.

  DECnet-DOS allows programmers to create C language and assembly language programs that use nontransparent task-to-task communication functions. C programs use socket interface calls to perform DECnet functions. DECnet-DOS also provides DECnet utility functions that allow you to access the network node database and manipulate the data.

  DECnet-DOS supports the DECnet-ULTRIX task-to-task network communications interface. Any DECnet-DOS C program using (compatible) DECnet-ULTRIX network interface calls can be transported easily to DECnet-ULTRIX systems.

  An assembly language program uses the MS-DOS interrupt function request (6EH) to request network process access. Information regarding I/O operations is passed with this MS-DOS function request. The information resides in either an I/O Control Block (IOCB) or a callback IOCB data structure.

Remote File Access and File Transfer

DECnet-DOS offers a set of utilities that allow a user to access network resources. Using the DECnet-DOS Transparent File Access (TFA) and Network File Transfer (NFT) utilities, you can transfer files between a PC and another node in the network. Transparent file access is also available to a DECnet-DOS task by adding network location information to an MS-DOS path-name string. Accessing remote files is accomplished with standard MS-DOS I/O system function requests.

You can use the TNT utility to display information regarding a TFA session. The TNT utility returns standard MS-DOS error messages and extended error messages that help locate problem areas.

The DECnet-DOS programming interface enables a programmer to issue calls to access a remote file. For most remote file operations, a call to access a file contains the following information:

- Remote file specification—The file specification identifies the remote file you wish to access. You must know how the file is identified by users on the node on which the file resides. Refer to the appropriate programmer's reference manual at the source or target systems for the correct file specification syntax.

- Access control information—Access control information contains arguments that identify the accessing program to the remote node. It consists of three character strings: a user identification name, a password associated with that user, and additional accounting information required by the remote system. This information must match the information in an account or guest account entry in the remote node's user file before your program can gain access to that node's resources.

▪ PCSA Server and Client Architecture

Figures 7-4 and 7-5 follow and show a conceptual view of the layered structure of the network.

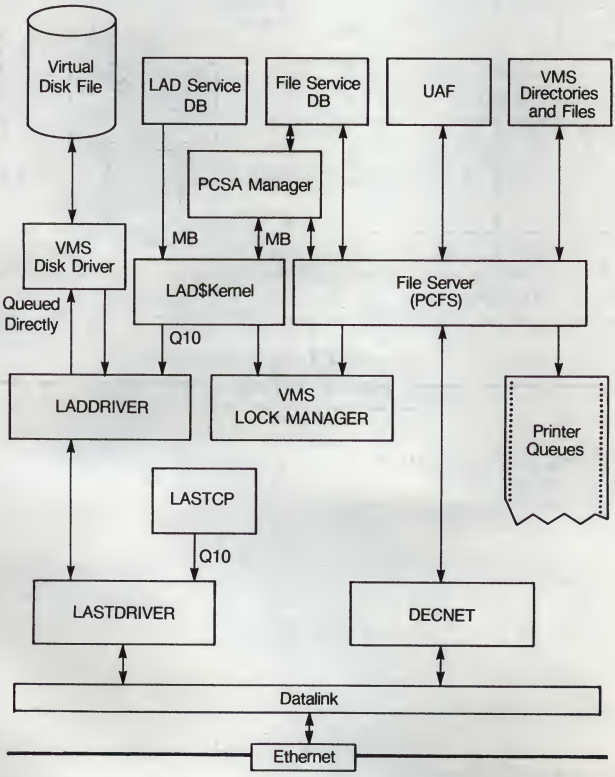


Figure 7-4 ▪ VAX/VMS Server Architecture

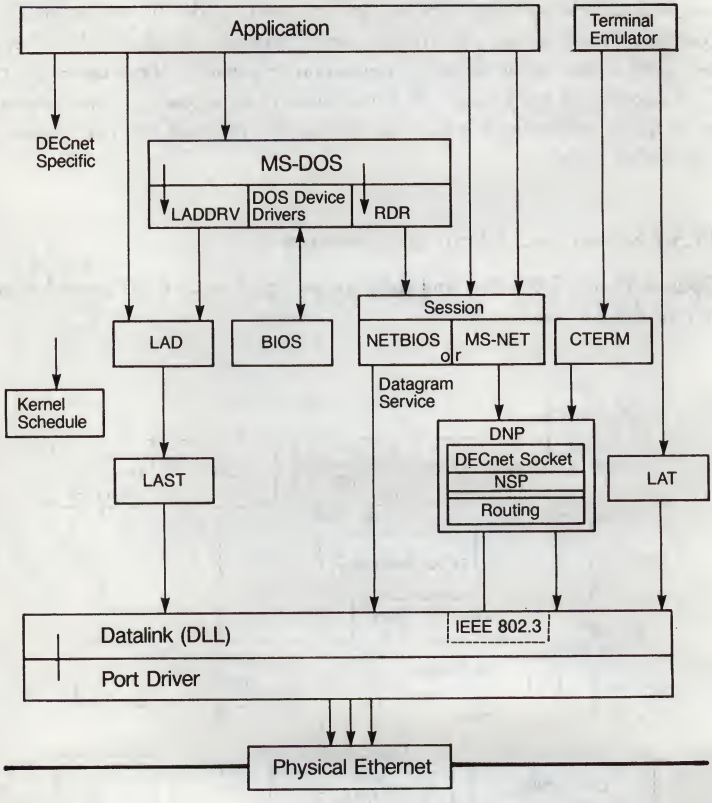


Figure 7-5 ▪ Client Architecture

Chapter 8 · The User Environment

With Digital's integrated personal computing products, PC users can continue to work with familiar desktop applications while taking advantage of the power of the corporate network. User-friendly interfaces, such as MS-Windows, are available to make the transition between the VAX/VMS and MS-DOS environments as transparent as possible. This chapter covers the user's environment, ways to use the network, and available tools for users.

· The MS-DOS Operating System

The DECnet/PCSA Client software integrates your version of MS-DOS. The MS-DOS operating system provides a command-line user interface to the applications and programs that run in the MS-DOS environment. Using MS-DOS commands, the user can perform a number of different tasks such as:

- Starting MS-Windows
- Connecting to network servers and services
- Printing files on either local or remote printers
- Creating, editing, copying, renaming, and deleting MS-DOS files stored in directories on diskettes, hard disks, virtual disks, and file service directories on a VAX/VMS server
- Running MS-DOS-based applications located on the PC workstation or on a server
- Creating programs to run in the MS-DOS environment or in MS-Windows

Table 8-1 shows Digital's DOS enhancements for PCSA MS-DOS. Digital also provides enhancements for other PCs.

Table 8-1 ▪ PCSA MS-DOS Enhancements from Digital

Command	Added Capability	Native MS-DOS
APPEND	Allows extension of current working directory.	Not available in MS-DOS V3.2.
BACKUP	Allows backup to network drives and to subdirectories.	MS-DOS V3.2 and V3.3 do not allow backups to subdirectories.
DECKEYB	Maps a specific character set to any keyboard, including international LK250 keyboards.	MS-DOS V3.2 and V3.3 only support industry-standard keyboards.
DECMODE	Allows for the setting of printer types, keyboardbuffer size, and bypass modem control.	Not available in MS-DOS V3.2 and V3.3.
GRAPHICS	Supports Digital printers: LN03 Plus, LN03 Plus with ISO PC cartridge, LA75, LA50, LA210, and LJ250.	MS-DOS V3.2 and V3.3 do not support Digital printers.
KEYBRD	Allows use of the extended ROM BIOS LK250 features with PC workstation.	MS-DOS V3.2 and V3.3 do not support the Digital LK250 keyboard.
MOUSE	Allows Digital mouse to emulate the Microsoft mouse.	MS-DOS V3.2 and V3.3 do not support Digital mouse as Microsoft mouse.
RESTORE	Allows user to restore files to a network drive and to subdirectories.	MS-DOS V3.2 and V3.3 do not allow files to be restored from subdirectories.
SHARE	Allows file sharing and locking.	MS-DOS V3.2 and V3.3 do not work with PCSA operating environment.
XONXOFF	Provides support for the XON/XOFF communications protocol required for most Digital printers.	MS-DOS V3.2 and V3.3 do not support the XON/XOFF communications protocol.

MS-DOS and VAX/VMS File Compatibility

The MS-DOS operating system and the VAX/VMS operating system have different file systems. While both have directory structures rooted on disk drives, their file-naming syntax differs.

When using the VAX/VMS operating system, you cannot create a file with the .DIR extension if a subdirectory with the same name already exists. For example, if the directory NAME exists, a file cannot be created called NAME.DIR.

File storage on the server can be an RMS sequential fixed-length record, as well as an RMS stream file.

Creating Files with Text Editors

Certain MS-DOS text editors end a text file with CTRL/Z as a delimiter. If such a file is created in an MS-DOS text editor and it needs to be used as a .COM file in the VAX/VMS environment, you have two options:

- Insert an **$ EXIT** as the last line of the **.COM file.**
- Edit the file on the VAX/VMS system and remove the **CTRL/Z.**

Files, created by a VAX/VMS text editor and to be used in the MS-DOS environment, are copied using the /A qualifier from the drive connected to the VAX/VMS server to any other drive. Copying the file (with the /A qualifier) removes any appended CTRL/Z characters. Certain MS-DOS application programs end abnormally when they encounter a CTRL/Z character.

Special Characters in File Names

Special characters are any valid MS-DOS file name characters other than A–Z, 0–9, $ and _ (underscore). Of the 11 characters that can be used in an MS-DOS file name and file extension, a maximum of 9 special characters is acceptable when creating a subdirectory.

The VAX/VMS server translates MS-DOS directory names with file extensions by treating the period (.) as a special character and appending .DIR as the file extension. For example, if a PC workstation user creates an MS-DOS directory named A.EXT, the directory is listed as A.EXT. However, the VAX/VMS operating system lists the directory as A__2EEXT.DIR.

Copying Binary Files Between MS-DOS and VAX/VMS Directories

MS-DOS binary files can be copied to a VAX/VMS directory using the MS-DOS COPY command. Any binary files that were not copied to the VAX/VMS directory with the MS-DOS COPY command should be copied to the MS-DOS environment with the NFT COPY command. For more information on NFT, see *Chapter 9* of this handbook.

Using MS-DOS Applications with VAX/VMS Created Files

Some MS-DOS applications (for example, EDLIN, the MS-DOS line editor) do not work with a file created by a VAX/VMS process. This is because the VAX/VMS server does not allow write access to those files. It does allow write access to VAX/VMS files with the stream record format but supports only read access to files with any other record format. Table 8-2 describes the VAX/VMS server support for MS-DOS access to VAX/VMS files.

Table 8-2 ▪ MS-DOS Access to VAX/VMS Files

If the VAX/VMS file record format is:	MS_DOS allows the user to:
Stream	Open Close Create Read Write/Append Delete
512-byte fixed-length record	Read Write Create
Sequential record	Open Read (sequential only)
Relative record	Open Read (sequential only)
Indexed record	Open Read (sequential only)

The VAX/VMS server supports only read access to ordinary Record Management Services (RMS) record files (nonstream files).

For word processing system (WPS) support, use 512-byte fixed-length records. For more information about creating this service, see the *VAX/VMS Services for MS-DOS Administration Guide.*

To convert a nonstream file to a stream file, copy the file to another file name.

▪ MS-Windows

DECnet/PCSA Client software includes Digital's adaptation of MS-Windows. MS-Windows provides a window-oriented user interface to MS-DOS and to the applications and programs that run in MS-DOS. With MS-Windows, users can display multiple tasks in different windows on the screen and switch between tasks with a mouse or keyboard. The drop-down menu, and the ability to switch applications using a mouse, means the user does not have to type many commands or memorize command formats. Figure 8-1 shows a typical MS-Window screen displaying multiple applications.

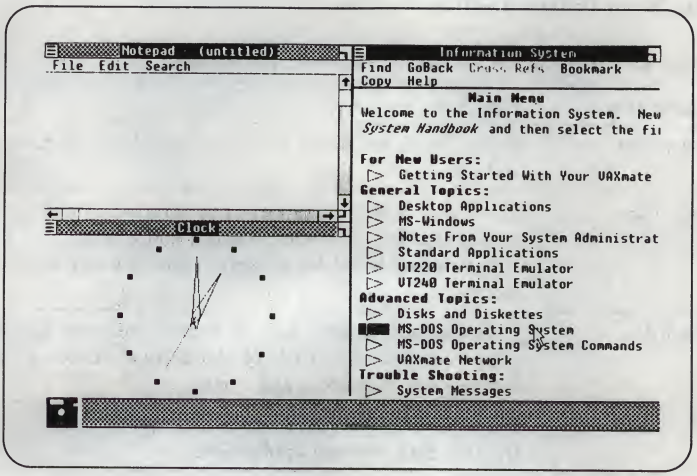


Figure 8-1 ▪ Sample MS-Window Screen

In addition to displaying multiple applications on the same screen, you also can perform many of the same tasks as from the MS-DOS prompt. With MS-Windows you can:

- Connect to the network servers and services
- Use the Configuration Aide to define PCSA network connections often made to automate the process of connecting to services
- Print files on either local or remote printers

- Create, edit, copy, rename, and delete MS-DOS files stored in directories on diskettes, hard disks, virtual disks, and file service directories on a VAX/VMS server
- Run applications stored on the PC workstation or a server
- Use the Notepad application to create programs to run in the MS-DOS environment or in MS-Windows

Some MS-DOS commands can be used only at the MS-DOS prompt. For more information, refer to the *MS-Windows User's Guide.*

The following desktop applications are included with MS-Windows. Table 8-3 lists the applications and their functions.

Table 8-3 ▪ Supplied MS-Windows Desktop Applications

Application	Function
Calculator	Works like a hand-held calculator with basic arithmetic and memory functions.
Calendar	Provides a desktop calendar or appointment book format that lets you enter, display, and edit appointments listed for a selected day of a selected month.
Cardfile	Organizes information such as names, addresses, and phone numbers into a file of alphabetical cards. Cards can be created, edited, and sorted.
Clipboard	Provides a cut-and-paste buffer that can be used to transfer data between applications.
Clock	Acts as a standard clock.
MS-Paint	Provides an application for creating, editing, saving, and printing artwork using icons instead of typing commands.
Notepad	Allows the user to display, create, and edit text files.
Reversi	Lets the user play a game against the PC workstation.
VT220	Lets you work with a host computer as if you were using a VT200 series terminal.

MS-Windows DECnet/PCSA Client Enhancements

Digital's DECnet/PCSA Client V2.0 software offers the following enhancements to MS-Windows:

- DEPCA mouse driver
- Format LAD drives
- Removable media devices
- Fragmentation solution

The DEPCA mouse driver supports the mouse attached to the DEPCA mouse port.

Format LAD drives means that Digital's DECnet/PCSA Client software can format virtual disk drives.

▪ Terminal Emulation

You can use your PC workstation as if it were a Digital terminal connected to a host computer. When a PC workstation is used to emulate a VAX/VMS terminal, you can perform standard terminal functions, access resources connected to the VAX host computer, use scripting for the terminal emulators, and use the Digital Multinational Character Set.

The SETHOST utility uses the following protocols:

- LAT (Digital's Local Area Transport) protocol that communicates only over the Ethernet. LAT supports Terminal Data Management System (TDMS) applications and can be used for sessions to nodes on the LAN.
- CTERM (Digital's Terminal Services Architecture Command protocol) is a wide-area virtual terminal protocol that is layered on top of DECnet. It is available for both Ethernet and asynchronous DDCMP configurations. CTERM does not provide support for TDMS applications, but does allow users to work with multiple sessions.

Terminal Emulation from MS-DOS

At an MS-DOS prompt, the SETHOST utility lets a PC workstation emulate a VT220 terminal and a VAXmate emulate a VT240 terminal. Each time the SETHOST utility is used to log into a VAX/VMS account, a network connection called a session is created. Users can create up to four consecutive sessions at once.

Terminal Emulation from MS-Windows

The VT220 terminal emulator is accessible from MS-Windows. The MS-Windows VT220 terminal emulator uses the LAT protocol for local area communications over the Ethernet by way of the serial communications port. The VT220 emulator application lets the user display the emulator in more than one window. Table 8-4 lists the features and differences between the styles of terminal emulation.

Table 8-4 • Terminal Emulation Functions

Function	VT220	SETHOST VAXmate (VT240)	SETHOST PC workstation (VT220)
Runs within MS-Windows	Y	N	N
Multiple sessions running	N*	Y	Y
Scripting	Y	Y	Y
ReGIS graphics	N	Y	N

* More than one VT220 application can be displayed in different windows. Each application is one session of the VT220 emulator.

DECnet/SNA MS-DOS 3270 Terminal Emulator V1.0

MS-DOS 3270 Terminal Emulator allows MS-DOS-based PCs running DECnet interactively to access IBM mainframe-based applications by the DECnet/SNA Gateway.

In typical 3270 operations, the IBM system transfers a formatted screen, much like a "form" or "panel" to the 3270 display, and the user fills in any data required by the form. The completed form is transmitted to the IBM host system as a single unit. This mechanism is emulated on the PC by buffering the form in memory on the PC and presenting it on the video screen. When the form is completed, the user sends it to the IBM system by the DECnet/SNA Gateway.

The key features of the 3270 Terminal Emulator are as follows:

- Since the MS-DOS 3270 Terminal Emulator is layered on top of DECnet for PCs, the user has direct access to both the Digital and IBM worlds from a single, networked PC.
- The IBM mainframe operating system support includes MVS, VM, and VSE/SP.

- The MS-DOS 3270 Terminal Emulator provides functions similar to those available for a user on an IBM 3178, 3180, 3278, or 3279 display station. A 3279 Base Color Support (text only) is included.
- An on-line HELP facility provides information about keyboard layout and functions associated with particular keys. The user can remap key functions onto different keys at any time.
- Ease of use is enhanced with capabilities that allow the user to switch between the DOS command line and a 3270 Terminal Emulation session.
- Ease of use is enhanced since frequently used key sequences can be associated with a particular Program Function Key so that pressing a single key can recall up to 127 keystrokes.
- Screen capture allows users to save the contents of a screen to a local PC file.
- Local and logical print capabilities allow users to place a screen of information onto hard copy.
- The customer can install the MS-DOS 3270 Terminal Emulation software using the step-by-step documentation available for this product.

▪ Accessing Services on the Network

The PCSA software includes network commands that let the user work with and manipulate the network connections. The user also can issue DECnet network commands.

Using PCSA and DECnet network commands, the user can connect to virtual disk services, file services, and printer services to create, use, delete, and print files over the network, as well as to control the use of network connections.

If a user frequently works with a particular virtual disk or printer service, the AUTOEXEC.BAT file can include the network commands to set it up automatically. Also, the user can connect to other resources available on the network.

For more information, refer to *Using Networks from Your PC Workstation.*

Chapter 9 • DECnet-DOS

DECnet/PCSA Client software is a superset of DECnet-DOS—that is, all features and programming tools included in DECnet-DOS are included in DECnet/PCSA Client as well. DECnet-DOS is also available as a separate PC connectivity product for PC users who require only (or primarily) task-to-task programming tools for customized applications or access to ULTRIX or RSX operating systems.

This chapter gives a brief overview of DECnet and discusses the main features of DECnet-DOS. These features also are available to users running the DECnet/PCSA Client software on their PC workstations.

• DECnet

DECnet is the name given to a family of software and hardware communications products that provide a network interface for operating systems. These products include:

- DECnet-VAX, used on VAX computers running VAX/VMS
- DECnet/RSX for PDP systems running RSX
- DECnet-ULTRIX for use on VAX computers running ULTRIX
- DECnet-DOS, used on IBM-compatible computers running MS-DOS

DECnet allows users to share information or exchange files between computers on a DECnet network. Individual systems (called nodes) in a network share resources and exchange information, files, and programs. Figure 9-1 shows a DECnet network.

The components in Figure 9-1 include:

- End nodes. An end node can receive and transmit information for its own use only. It cannot receive and then automatically forward information intended for other nodes.
- Local nodes. A local node is any node you physically use to enter commands.

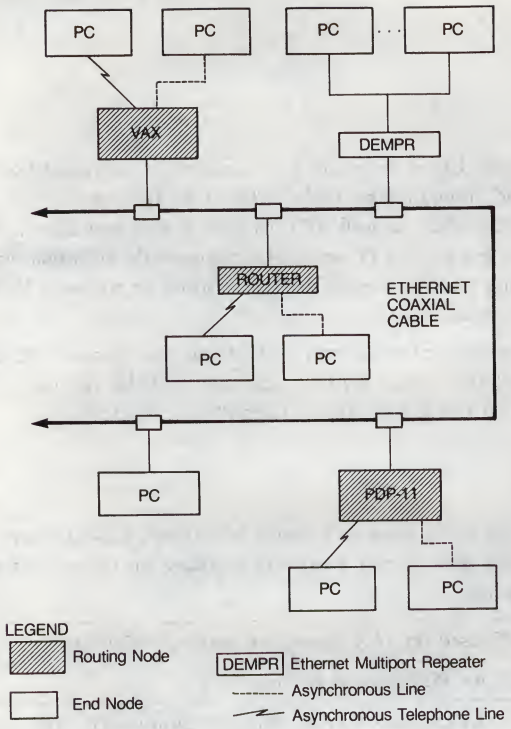


Figure 9-1 ▪ A Sample DECnet Network Configuration

- Executor nodes. An executor node performs network management functions. This node enables users to obtain information about the network.
- Remote nodes. From the vantage point of the PC shown in Figure 9-1, the other network nodes are remote nodes.
- Adjacent nodes. An adjacent node is physically connected to a local node by a single line.
- Routing node. A routing node automatically forwards information, files, and programs between other nodes in the network. This allows an end node to copy data to and from any other node in the network.

▪ DECnet-DOS

DECnet-DOS is the product name for a set of software products that allow IBM systems and IBM-compatible systems to connect to a DECnet network.

DECnet enables individual computer systems or PCs to communicate effectively with one another in a network. Using DECnet-DOS, your PC can communicate with VAX computers, PDP-11 computers, DECsystem 10s, DECSYSTEM-20s, and any other system that uses DECnet.

A DECnet-DOS node can be used in two environments:

- WAN. As an asynchronous DDCMP DECnet end node, using the asynchronous serial communications port
- LAN. As an Ethernet end node, using a Digital or vendor-supplied Ethernet controller board and Ethernet hardware to connect to a LAN

▪ DECnet-DOS Capabilities

DECnet-DOS provides the following network capabilities:

- Network management, which allows you to control, monitor, and test DECnet-DOS software. You can reconfigure your network node as the need arises.
- Remote file access, which allows you to access files on remote nodes. You can store and retrieve information on remote nodes. By storing the most current version of a file on a remote node, you eliminate the need for keeping a version of the file on each node.
- Bidirectional file transfer, which allows you to exchange files with other nodes. This speeds the information flow between organizations and decreases the paperwork.
- Resource sharing, which eliminates the need for duplicating resources at each node. With resource sharing, many nodes can use the same printers, storage facilities, and processing capabilities.
- Resource server functions, which provide services to other nodes in the network (file storage, for example).
- Mail, which allows you to send messages and files to users on other nodes.
- Task-to-task communication, which allows data exchange between programs without human intervention. DECnet allows programs that are running under different operating systems and written in different languages to communicate. These customized applications can use DECnet in a manner totally transparent to the user.

- File Access Listener (FAL), which allows other DECnet nodes to gain access to the files on your DECnet node. In addition, FAL is required for other nodes to copy files to your PC.
- Job Spawner, which allows you to run multiple processes.
- NETBIOS, an industry-standard session-level interface used with some third-party applications to provide support for adapter names and datagrams.
- SETHOST, which supports terminal emulation by LAT and CTERM, for WAN and LAN virtual terminal capabilities.

▪ Operating DECnet-DOS

The DECnet protocols require that messages be sent and received even when network applications are not running. This includes, for example, periodic tests of the line to determine that it is still operational.

Since MS-DOS is not a multitasking operating system, special efforts must be taken to allow network processing to occur while an application is running in the foreground. The DECnet Scheduler (SCH) component provides this special effort by managing interrupts and regulating the use of the system clock.

For asynchronous configurations, the DECnet Network Process (DNP) component provides all network services, including processing of all requests for performing network operations and background networking tasks.

For Ethernet configurations, both DECnet and the LAT must use the Ethernet simultaneously. To do this, the Data Link Layer (DLL) network component handles all transmission and reception of messages on the Ethernet. The DNP component communicates with the DLL to provide all DECnet services. The LAT component cooperates with the DLL to provide LAT services for the SETHOST utility.

For efficient use of the network components (SCH, DNP, and DLL), DECnet provides both a user interface for performing network functions and an applications programming interface for creating applications programs. User programs and applications development provide remote file access services and task-to-task logical link support. These services allow for both nontransparent and transparent task-to-task communications. Programmers can write nontransparent communications programs in either C language or assembly language. Transparent communication programs can be written in any of the higher-level languages.

Asynchronous DDCMP Communications

You can add a PC to the network by connecting it to an adjacent routing node using asynchronous DDCMP communications. To connect your DECnet-DOS node to an adjacent routing node you perform the following steps:

1. Select an adjacent node. The selected routing node must be one of the following Phase IV or Phase V routing nodes capable of supporting asynchronous DDCMP lines:
   - VAX/VMS V4.2 or later
   - RSX-11M V4.2 or later
   - RSX-11S V4.2 or later
   - RSX-11M-PLUS V3.0 or later
   - DECrouter 200 V1.0 or later
2. Install appropriate hardware. The required hardware components include:
   - Asynchronous communications adapter
   - Asynchronous communications adapter cable
   - Modem, pair of modems, or a null modem/null modem cable
3. Configure the adjacent node. The DECnet product at the adjacent node must support asynchronous DECnet communication.

Ethernet Communications

You also can add your PC to the network by connecting it directly to the baseband Ethernet LAN. An Ethernet connection scheme is possible using an Ethernet interface. To connect your DECnet node directly to the baseband Ethernet:

1. Select a communications adapter. Choose one of the following supported adapters:
   - Digital DEPCA Ethernet Controller Adapter
   - 3COM Etherlink/II and 3COM Etherlink/MC
   - MICOM NI5010-1 and NI5010-2
2. Configure hardware options. Configure the communications adapter to run DECnet-DOS software as follows:
   - I/O address = 300 (hex)
   - Interrupt request = 3
   - DMA request and acknowledge = 1

3. Install the appropriate hardware. You must install the following hardware components:
   - Ethernet communications adapter
   - Ethernet cable
   - Ethernet connector

▪ Installing DECnet-DOS Software

This is only necessary for standalone PC workstations that are not using the PCSA Client software.

DECnet-DOS offers an automated installation procedure for both the experienced and the inexperienced user. The DECnet Installation Procedure (DIP) makes it easy to install DECnet software on a PC:

- First, DIP automatically checks to see whether your PC is configured properly (operating system, sufficient memory, and disk space). Next, DIP guides you through the installation by asking for your responses to a set of questions and a series of menus. Your answers are used to configure your network parameters and install selected DECnet utilities.
- DIP also automatically tailors your system startup files (AUTOEXEC.BAT and CONFIG.SYS) by adding command lines to automatically execute (or load) DECnet modules when your operating system is started. These modules—the DECnet Network Process (DNP), the Data Link Layer (DLL), and the Real-Time Scheduler (SCH)—access DECnet database files and drive the DECnet-DOS software.

Selecting DECnet Utilities

Any supported PC with 512Kb of memory can run DECnet-DOS software. The DECnet-DOS software kit consists of many separate components that enable you to perform high-level network functions. The minimum set of these DECnet-DOS components run DECnet and require memory as follows:

- For Ethernet communications the SCH, DNP, and DLL make up the minimum DECnet configuration and require approximately 126Kb of the available 512Kb of memory.
- For asynchronous communications the SCH and DNP make up the minimum DECnet configuration and require approximately 70Kb of the available 512Kb of memory.

The remaining memory is available for your operating system, a minimal subset of DECnet utilities, and other non-DECnet applications such as word processing or spreadsheet packages running on your PC.

When installing DECnet software, you can install all of the optional components or you can select individual DECnet utilities. Your choice depends on how the system is configured (hard- or floppy-disk based), whether there is sufficient disk and memory space, and what network functions you wish to access. Table 9-1 lists network functions, their corresponding DECnet components, and the approximate memory requirements for each utility.

Table 9-1 ▪ DECnet Utilities and Required Memory

Network Function	DECnet Utility	Memory
Network management	Network Control Program (NCP)	102Kb
Remote file access	Transparent File Access (TFA)	47Kb*
	Network File Transfer (NFT)	110Kb
	Mail	86Kb
Network virtual terminal	SETHOST	188Kb
	Local Area Transport (LAT)	12Kb*
	Network Virtual Disk Driver (NDDRV)	8Kb†
Resource sharing	Network Virtual Printer Driver (NPDRV)	7Kb†
	Job Spawner	24Kb
	File Access Listener (FAL)	60Kb
	windows version	72Kb
	Network Disk Utility (NDU)	57Kb
Network programming	Programming Interface Library	—
	Transparent Task-to-Task (TTT)	23Kb*

* Resident in memory; may be installed at any time.

† Resident in memory; must be installed at boot time.

Any of the DECnet utilities can be started from the MS-Windows environment. NFT and FAL operate as Class A applications, which means they are fully functional in the windows environment. NDU and the Job Spawner operate as Class B applications, which means they work as if you started them from the command line, but they appear as part of a window. SETHOST operates as a Class C application, which means that even though you start a utility from a window, it takes over the entire screen and the windows are no longer visible. When you exit from a Class C application, you are returned to the previous window environment.

TFA, LAT, and TTT are programs that terminate and stay resident (TSR). NDDRV and NPDVR are device drivers (DD). The window classifications do not apply to TSR and DD programs.

▪ Verifying Your Installation

DECnet-DOS also enables you to verify installation. After completing the software installation, NCP configures your DECnet node. You can run these tests manually or have them run automatically as part of the installation procedure. If you run the tests automatically, the installation procedure prompts you for the specific address of at least one reachable remote node to use for testing.

▪ Utilities for Network Management

DECnet-DOS provides two utilities that allow you to manage your network node: Network Control Program (NCP) and the Network Management Listener (NML).

Network Control Program
The NCP performs three primary functions:

- Displays statistical and error information
- Controls the node's network components
- Tests local network components

The output resulting from a command can be directed to a local file or to the PC console.

The user can display the status of the local node's DECnet activity. Statistics related to both the node and the communication line can be displayed, including data on traffic and errors. Network parameters such as line speed, timer values, and buffer sizes can be modified. Control functions are limited to starting and stopping the line and activating the local node. In order to test hardware components, test messages can be sent and received over the line either between the PC workstation and adjacent node, or through controller or modem loopback arrangements.

By starting with your local node and progressing outward to each of the components in your network, you can determine which component is not operating properly.

NCP lets you use loop messages to test the following parts of your network:

- The local node
- A turnaround connector on the line or controller
- A local or remote modem (for DDCMP use only)
- An adjacent node at the circuit level (for DDCMP use only)
- A remote node at the circuit level (for Ethernet only)
- A remote node at the application level

The loop tests are performed using the following information:

- The length of the test message
- The number of times to send the test message
- The type of format for the test message
- The node that will receive the test message and transmit it back to your node

DECnet-DOS provides for limited local network event logging. Network management requests from remote command nodes are not responded to by the DECnet-DOS system, unless NML is running. However, the NCP program can act as a loopback mirror to which remote nodes can send test messages for diagnostic purposes.

Network Management Listener

The Network Management Listener task is an optional background task that allows remote DECnet nodes to monitor network activity and parameters on DECnet-DOS nodes. This allows network managers to determine whether or not remote DECnet-DOS nodes are functioning correctly on the network. Remote alteration of the network parameters is not supported.

• DECnet Utilities for Remote File Access and File Transfer

DECnet provides two utilities that allow you to manipulate files by accessing them remotely and/or transferring them to and from remote nodes: NFT utility and FAL utility.

Network File Transfer Utility

The NFT utility allows you to perform several tasks:

- Append two or more files
- Copy files between local and remote nodes (ASCII and binary)
- Delete local and remote files
- List files located on a local or remote directory
- Define and display access control information
- Run batch (or command) files on remote nodes
- Display the contents of a local or a remote file on your screen
- Print files on remote printers

NFT can perform these functions between any two DECnet nodes. They do not have to both be PCs; for example, one node can be a PC and the other a VAX computer.

File Access Listener

The FAL enables you to let other nodes access files on your node. The purpose of the FAL utility is to listen for and receive remote access requests from the network. These requests result from file access routines from other nodes in the network such as an NDU OPEN command from another MS-DOS node or a dcopy\ command from a DECnet-ULTRIX system. When FAL detects a request to copy a file to or from your node, it first checks the type of access privilege contained in the request. If it has the proper privilege for access to your node, FAL sends or receives the file data to or from the requesting node. (Access information is specified and displayed using NCP commands SET ACCESS and SHOW KNOWN ACCESS.)

FAL can accept requests from multiple nodes simultaneously. The number of multiple requests that FAL can accept depends on the maximum logical links you have defined with the NCP command, SET MAXIMUM LINKS.

FAL must be running on your system or must be run by the Job Spawner before any exchanges of file data can take place. While FAL is running, file data is passed back and forth between your node and the requesting node(s). You can control data conversion during file transfers using the switches listed in Table 9-2.

Table 9-2 ▪ Switches for Control of Data Conversion During File Transfers

Switch	Meaning
ASCII (/A)	All files copied from the PC are transferred as ASCII files.
BINARY (/B)	All files copied from the PC are transferred as binary files.
ERROR (/E)	Causes FAL to report an error to the remote node if the requesting node is attempting to overwrite an existing file. If this switch is not set, an existing file will be deleted and a new one will be created with the same name.
LOG (/L)	Causes FAL to log the type of access for every request it receives. The type of access includes: the command or request (such as an NFT DIRECTORY or DELETE command); the requested directory name and file name; the node name; and the access control information for that node (user name and account).

▪ The DECnet-DOS Mail Utility

The DECnet-DOS Mail Utility lets you send messages and text files to other nodes in the network. This utility allows you to simply enter the MAIL command and include a subject, file name, and address. You can edit MAIL files before sending them, and you can add qualifiers directly on the MAIL command line. MAIL allows you to work with the editor of your choice.

▪ DECnet-DOS Utility for Virtual Terminal Operations

The DECnet SETHOST utility provides the user with VT220 terminal emulation by LAT, CTERM, or the asynchronous serial communications port. SETHOST allows the PC to appear as if it were a terminal physically connected to the target system. This is particularly useful for remote program development because it allows the user of the small, application-oriented PC to use the resources of larger systems.

A maximum of four SETHOST sessions can be enabled simultaneously, by LAT or CTERM. With a single keystroke, the user can switch among active SETHOST sessions. Only one session can be enabled when SETHOST uses the asynchronous communication port for an asynchronous terminal connection. With a single keystroke, the user can leave an active SETHOST session and return to the DOS environment. To return to the SETHOST session, the user simply types EXIT at the DOS prompt. Multiple CTERM and LAT terminal sessions (to the same or different hosts) can be established, suspended, and resumed.

Terminal characteristics can be selected and saved with the utility's setup feature. The following character sets are supported with SETHOST: ISO Latin-1 (ISO), DEC multinational (MCS) and National Replacement (NRCS).

Full local printer support is provided under SETHOST (that is, printing within ALL-IN-1) with Digital printers. SETHOST sessions also can be logged to a file for future examination. SETHOST supports control of an asynchronous modem.

SETHOST provides a script processing language that allows the automation of frequently executed functions. For example, a script can be written automatically to log a user in to a computer or to dial in to a computer and establish a DDCMP connection. Scripts can be written that perform a task and then exit SETHOST, without user intervention.

▪ DECnet-DOS Utilities for Resource Sharing

DECnet-DOS provides several utilities for sharing network resources. These utilities include the following:

- NDU, which controls your use of remote printers and remote disks
- FAL, which lets users access files and disks on your node
- Job Spawner, which allows your PC to act as a server for performing multiple service functions

Network Device Utility

The NDU controls remote printers and disks as if they were directly connected to your PC. The disk or printer resident on the remote node appears to be a local device, except for differences in access time. These differences depend on the type of communication services that exist on the remote node you are using.

A remote disk file can be assigned a volume name (such as G:) and can be used by MS-DOS utilities or applications software as if it were a local hard-disk volume. A remote printer is assigned the device name NPRN and can be used like a local printer. Since the device only appears to be resident at the local node, it is called a virtual device.

With NDU, you can perform the following tasks:

- Assign a hard-disk volume name to a new or existing remote file to be used as a virtual disk volume
- Stop the use of a remote file as a virtual disk volume
- Delete a remote disk file that had been used as a virtual disk volume
- Assign the printer device name NPRN to a disk file at a remote node
- Stop the use of the virtual printer at the remote node and save the text file to be queued for printing
- Obtain status information about all assigned hard-disk drives, printer devices, and command default values

NDU controls the use of both virtual disks and virtual printers:

- Virtual disk volumes. NDU allows you to access up to four virtual disk volumes at once. You can access four volumes on the same remote node, one volume on each of four different remote nodes, or any other combination totaling four volumes. Each remote volume is a file that is treated as if it were a hard disk. The file is a binary file on the remote node that contains MS-DOS directories and files.

  Virtual disks can be 1, 10, 20, or 32Mbs. The operating mode for these disks is either RO or RW. RO means that the disk can be shared, but only for read access. RW means that the disk can be read from or written to, but cannot be shared. The default is RW.

- Virtual printers. NDU allows you to access one virtual printer at a time. The remote node that provides the virtual printer saves any text you output to the printer device NPRN in a temporary file. When you stop using the virtual printer, the temporary file is queued to the default printer on the remote node.

Job Spawner

The Job Spawner allows your computer to act as a server for performing multiple service functions. When you turn on the Job Spawner, it listens for any connection requests from other nodes in the network. When a connection arrives, the spawner starts the program that will service that request. When the service is complete, the spawner again waits for connections. In this way, your PC can process different requests at different times without any need for user intervention.

For example, if the Job Spawner detects a request for file transfer, the spawner initiates the FAL utility and causes FAL to run. FAL will continue to run until the requested activity is complete. The spawner then continues to listen for other requests or services. Note that two service programs cannot be run simultaneously.

With DECnet, the Job Spawner supports both FAL and the DECnet Test Receiver (DTR) utilities. User-written network applications also can take advantage of the Job Spawner.

To tell the spawner which programs to run for each kind of connection that arrives, the user must create the file DECSPAWN.DAT. Any editor installed on the local system can be used. The DECSPAWN.DAT file is an ASCII text file used as a database by the spawner.

Chapter 10 · International Character Sets and Keyboard Support

The PCSA product supports the use of several character sets. This chapter describes the character sets and how their implementation differs in MS-DOS and MS-Windows.

The system administrator can customize the MS-DOS and MS-Windows environments to support items such as the country keyboard, preferred character set, and preferred country information.

· International Character Sets

PCSA supports use of the following character sets:

- Digital Multinational Character Set (MCS). Digital developed this 8-bit character set. It includes the majority of the characters required for most of the Western European languages.
- ISO Latin-1. The ISO developed this 8-bit character set developed for Western European languages. It is similar to the Digital MCS.
- Industry-Standard Extended. This is an 8-bit industry-standard character set, of which PCSA supports two variants: Industry-Standard Extended and Industry-Standard Norway and Denmark Extended. The first variant includes those characters required for all Western European languages except Norway and Denmark. The second variant includes the character requirements for Norway and Denmark. Within PCSA, the first variant is known as STD, and the second variant as ST2.
- National Replacement Character Set (NRC). This 7-bit character set replaces a number of less commonly used symbols with national characters. Different countries use different variants of this character set. Each country therefore has its own National Replacement Character Set.

Within PCSA, implementing these character sets differs, depending on whether they are being used with MS-DOS or MS-Windows. Table 10-1 summarizes how the character sets are supported.

Table 10-1 ▪ Support of Character Sets

Environment	Character Sets Supported
MS-Windows	ISO (default) (STD/ST2) (MCS) (NRC)
MS-DOS	STD/ST2

In both MS-DOS and MS-Windows, multinational characters should not be used in file names.

▪ Character Sets in MS-DOS

When working within MS-DOS, the default character set (held in RAM) is Industry-Standard Extended. Users can set up a preferred character set (NRC, ISO, MCS) on the system using the MS-DOS DECKEYB and FONT commands. If this option is chosen, the character set and keyboard driver must be compatible.

▪ Character Sets in MS-Windows

When working within MS-Windows, the character set varies, depending on how the application interacts with MS-Windows.

- Applications developed specifically for use with MS-Windows (for example, Notepad, Paint, MS-DOS Executive) default to the ISO character set.
- Applications developed for MS-DOS, but which run in a Window (for example, COMMAND.COM), use the Industry-Standard Extended character set.
- Applications that do not run in a window (for example, the MS-BASIC Compiler) use the character set that was last loaded by MS-DOS.
- Other applications may use their own character sets.

▪ Customization of Country Information

The MS-DOS and MS-Windows environments are shipped with default settings. The MS-DOS environment defaults to industry-standard requirements, and MS-Windows defaults to the country requirements. The following defaults can be reset in MS-DOS:

- Keyboard
- Country format information (date, time, number, currency)
- Graphics information

These defaults can be reset in MS-Windows:

- Keyboard
- Country format information using the control panel.

▪ Supported Character Sets and Keyboards

Table 10-2 lists the complete set of supported character sets.

Table 10-2 ▪ Supported Character Sets

Digital Multinational Character Set
Finnish 7-Bit National Replacement Character Set
French-Canadian 7-Bit National Replacement Character Set
French 7-Bit National Replacement Character Set
German 7-Bit National Replacement Character Set
ISO Latin-1 Character Set
Italian 7-Bit National Replacement Character Set
Norwegian/Danish 7-Bit National Replacement Character Set
Spanish 7-Bit National Replacement Character Set
STD Character Set
ST2 Character set
Swedish 7-Bit National Replacement Character Set
Swiss 7-Bit National Replacement Character Set
U.K. 7-Bit National Replacement Character Set

Table 10-3 lists the country keyboards that are supported.

Table 10-3 • Supported Keyboards

Canadian-English Keyboard
Danish Keyboard
Finnish Keyboard
French Keyboard
German/Austrian Keyboard
Italian Keyboard
Norwegian Keyboard
Spanish Keyboard
Swedish Keyboard
Swiss-French Keyboard
Swiss-German Keyboard
US/UK Keyboard

Chapter 11 · Integrated Personal Computing Resources

This chapter contains many of the PCSA resources available to Digital customers. These resources include documentation, SPDs, service information, brochures, and other promotional materials. (Order numbers for some products are given in parentheses after product names.)

· PCSA Product Kits

This is an overview of the documentation provided for all users. It includes a brief summary of the purpose of the books in each set and explains where users can find specific types of information.

The basic PCSA product kits fall into the following categories:

- Server kits:
  - VAX/VMS Services for MS-DOS
- Client kits:
  - PC Client installed using VAX/VMS media
  - PC Client using 5 1/4" MS-DOS diskettes
  - PC Client using 3 1/2" MS-DOS diskettes

Each server kit includes a manual with instructions for installing the server software.

The specific manual Digital supplies depends on the type of Client software being installed. The installation manuals are intended for system administrators and should be added to the system administration documentation binder.

Additional documentation for programmers and system designers is available separately from the PCSA documentation sets.

· PCSA Starter and Integration Kits

To provide cost-effective entry-level PC integration solutions for customers and maintain a high customer satisfaction level, Digital offers two kits:

- DECnet/PCSA Starter Kits
- PC Workstation Network Integration Kits

The DECnet/PCSA Starter Kit combines individual products into a single package. The package includes these components:

- DEPCA-BA Ethernet controllers (4)
- VSXXX-AA mouse (1)
- VAX/VMS Service for MS-DOS media and documentation (1)
- DECnet PCSA/Client software media and documentation (1)
- DECstart service (1)

The PC Workstation Network Integration Kit provides a DEPCA board required to connect the PCs to an Ethernet network. The DEPCA is available with either a ThinWire Ethernet cable assembly or a standard Ethernet cable assembly.

Each Network Integration Kit includes these components:

- DECnet/PCSA Client license
- DEPCA board
- ThinWire Assembly Kit (with ThinWire Ethernet cables, T-connectors, and terminator)
- Digital mouse (DEPCA-K kit only)
- Digital keyboard (DEPCA-K kit only)

These kits were designed to help simplify the process of integrating your PCs into the larger corporate network.

• Administrator Documentation

The documentation for the VAX/VMS server administrator provides task-oriented and reference information.

The VAX/VMS server administrator should have experience with the following software and tasks:

- VAX/VMS operating environment
- VAX/VMS system management
- MS-DOS operating system
- DECnet network and network concepts
- DECnet network management and control

Table 11-1 lists information the system administrator can find in each of the manuals included in the set.

Table 11-1 ▪ VAX/VMS Services Administration Documentation Set

Title	Contents
VAX/VMS Services for MS-DOS Installation Guide	Provides information about installing the VAX/VMS services, including information for upgrading VAX/VMS services software already installed on your server
VAX/VMS Services for MS-DOS Administration Guide	Provides instruction and reference information about configuring and managing the disk and file services, using the PCSA_ADMIN and PCSA_MANAGER utilities, and the LAST Control Program
Network Troubleshooting Guide	Provides information about how to find and correct problems with the ThinWire Ethernet network components, installation procedures, and the DECnet/PCSA network

In addition, the following guides in the client documentation kits are useful to the system administrator. These guides include:

- Client installation guides. Intended for the system administrator. Provide information on installing DECnet/PCSA Client software.
- *Using Networks from Your PC Workstation.* Provides information about using the network.
- *DECnet-DOS User's Guide.* Provides information about using the DECnet network.
- *DECnet-DOS Network Management Guide.* Provides information about managing the DECnet network.

▪ Client Documentation

The documentation for client users is organized by PC workstation and media. The PC Client kit includes the following client installation guides:

- *Installing DECnet/PCSA Client with 3 1/2" MS-DOS Diskettes*
- *Installing DECnet/PCSA Client with 5 1/4" MS-DOS Diskettes*

The installation guides are written for system administrators and should be added to the system administrator's documentation binder.

Documentation for PC workstation users provides task-oriented and reference information. Users have varying levels of expertise, and they may be:

- New to computers
- New to a windowing environment
- Experienced using MS-Windows
- Experienced MS-DOS users
- New to working in a network environment
- Experienced with networking

A system handbook *Personal Workstation Handbook* is packaged with your PC client kit.

Table 11-2 lists information PC workstation users can find in each of the manuals included in the set.

Table 11-2 • Client User Documentation

Title/Topic	Description	Audience
Introductory Information		
PC workstation	Introduces you to Digital's personal PC workstation network, accessible with the Network Installation. Teaches basic skills for using the personal PC workstation network, MS-Windows, and the Information System.	PC client users who are new to computers and to desktop PCs.
Overview	Introduces the PCSA network environment, including general concepts and information about the servers and the services they provide, clients and client software, configuring a PCSA network, and site planning.	New users and system administrators, or anyone interested in an overview of the PCSA system.

Table 11-2 ▪ Client User Documentation (Continued)

Title/Topic	Description	Audience
MS-Windows, MS-DOS, and Printing		
MS-Windows User's Guide	Introduces you to MS-Windows and provides easy-to-access reference information. Includes information about using the mouse and the keyboard, configuring the PC workstation, and using applications.	New and experienced MS-Windows users.
MS-DOS Reference Manual	Covers MS-DOS commands and utilities for the PC workstation. Includes information about using the MS-DOS operating system and directory structure.	Any PC workstation user.
MS-DOS Enhancements	Covers special MS-DOS commands and utilities modified to work in the PCSA environment.	Experienced users. This book is not a tutorial.
Printing Guide	Provides advanced information about changing PC workstation printing configurations for MS-Windows and MS-DOS. Also, tells about how to print using local or remote printers from MS-Windows and MS-DOS.	PC workstation users with MS-Windows and MS-DOS experience who want to change the printing configurations set up by their system administrators.
Client On-line Information System	Provides instructions and reference information about using MS-Windows, MS-Windows applications, the MS-DOS operating system, and network commands.	Any PC workstation user.

Table 11-2 ▪ Client User Documentation (Continued)

Title/Topic	Description	Audience
Configuring the PC Workstation and Using the Network		
Using Networks from Your PC Workstation	Provides instructions for configuring your workstation to use the remote boot feature of a VAX/VMS server and to use the PCSA network. It also includes reference information about network user commands.	PC workstations users and system administrators with MS-Windows and MS-DOS experience. Experience using networks is not necessary.
DECnet-DOS Documentation	Guides from the DECnet-DOS documentation set. Includes information on using the SETHOST feature.	PC workstation users with MS-Windows and MS-DOS experience. Users interested in information using the SETHOST feature. Experience using the Digital DECnet network is helpful.
Customizing Your PC workstation to Conform with International Conventions		
International Features Guide	Provides information about how to customize the MS-DOS and MS_Windows environments to support such items as country keyboards, character sets, and date and time formats.	Any user whose PC workstation configuration must conform to international conventions.

▪ DECnet-DOS Information

For the complete and current ordering information refer to the DECnet-DOS SPD. For further information about DECnet-DOS, refer to the following documentation:

- *DECnet-DOS Installation Guide.* Details the procedures for installing DECnet-DOS on the IBM PCs (IBM Personal Computers PC, XT, and AT). This guide describes the configuration of the networking hardware, including jumper settings to use with the Ethernet interfaces.
- *DECnet-DOS Getting Started.* Provides an overview of the basic tasks that can be performed over the DECnet network. It introduces frequently used DECnet-DOS commands.
- *DECnet-DOS User's Guide.* Describes how to use the DECnet-DOS utilities. It details the DECnet-DOS commands used for performing network tasks.
- *DECnet-DOS Programmer's Reference Manual.* Details the network programming calls used in the creation of DECnet-DOS applications. This manual is designed for applications developers who are responsible for creating DECnet-DOS applications.

For more information about DECnet and DECnet products, read the following publications:

- *DECnet Digital Network Architecture (Phase IV)* (AA-N149A-TC)
- *Digital's Networks: An Architecture with a Future* (EB-26013-42)
- *Overview of Digital Networking Products* (AA-X104A-TK)
- *Network and Communications Buyer's Guide* (ED-31664-42)

Books can be ordered separately from the kits. When ordering sets of additional books, remember to order binders. The binders are not included when books are ordered separately from the kits.

▪ PCLAN/Server V1.0 Documentation

- *Release Notes, V1.0* (AA-MA12A-TE)
- *Mandatory Update Release Notes, Version 1.0A* (AV-MI96A-TE)
- *Personal Workstation Handbook* (ED-DEPCA-UG-0012)
- *Installation Guide* (AA-MA10A-TE)
- *Server Setup and Management Guide* (AA-MA11A-TE)
- *VAX/VMS Services for MS-DOS Administration Guide* (AA-JU51B-TE)

- *Network Troubleshooting Guide* (AA-JU54B-TH)
- *MS-DOS Reference Manual* (AA-LB62A-TE)
- *MS-Windows User's Guide* (AA-LB57A-TH)
- *PC-MAIL User's Guide* (AA-MA14A-TE)
- *SEDT User's Guide* (AA-MA13A-TE)
- *Printing Guide* (AA-KY01B-TH)
- *International Features Guide* (AA-LD51A-TH)
- *DOS Enhancements* (AA-JU55B-TH)
- *Using Networks from Your Workstation* (AA-MA16A-TE)
- *DECnet-DOS Getting Started* (AA-EV70C-TV)
- *DECnet-DOS User's Guide* (AA-EB45C-TV)
- *DECnet-DOS Network Management Guide* (AA-EV70C-TV)
- *DECnet-DOS Programmer's Reference Guide* (AA-EB46C-TV)
- *VMS General User's Manual* (AA-LA98A-TE)
- *VMS System Manager's Manual* (AA-LA00A-TE)
- *VMS Mini-Reference* (AA-LA96A-TE)
- *VMS License Management Utility Manual* (AA-LA33A-TE)

▪ Software Product Descriptions

SPDs are the official defining documents for Digital licensed software products. An SPD describes all important functional characteristics of a product in clear and concise language. The terms and conditions under which the corporation sells and licenses its software products identifies SPDs as the documents that specify Digital's obligation under software warranty. They describe a software product's system environment and identify required and optional hardware and software. The SPDs also provide the ordering information and identify any additional services available.

The XX stands for the revision number. By specifying the XX you will be sent the latest version of that SPD.

The SPDs for PCSA and associated Digital products are:

- *DECnet-DOS V2.1* SPD 50.15.04
- *DECnet/PCSA Client: PC V2.1* SPD 55.07.04 (formerly *PCSA/PC Client*)
- *DECrouter 200 V1.0* SPD 27.72.01

- *DECnet/SNA MS-DOS 3270 Terminal Emulator, V1.0* SPD 30.63.00
- *PCLAN/Server 2000* SPD 55.D1.xx
- *VAX/VMS Services for MS-DOS V2.1* SPD 30.50.03, SPD 30.50.03-A

SPDs are available from a local Digital sales representative.

▪ Service

Digital's prerequisite PCSA DECstart Service provides implementation support for installing VAX/VMS Services for MS-DOS on the first server at a customer site. The service includes a survey of the customer's needs, installation and set up of the server, server-based MS-DOS applications, and the client software on a DECnet network. It also includes a briefing of the system administrator on operation of the server and its associated group of PCs, and orientation for PC users. In Europe, this startup consulting service is called MS-DOS SERVERstart.

Digital also offers Self-Maintenance, Basic Support, and DECsupport for VAX/VMS Services for MS-DOS. Optional hardware installation is also available.

▪ The Digital Service Solution

With a worldwide Field Service force of 27,000 and 14 worldwide customer support centers, Digital Equipment Corporation can provide much more than remedial hardware fixes.

In today's business environment, the PC rarely stands alone. Most computing environments are networked, and there is a growing trend to incorporate many vendors' products into a customer's solution. Through our DECcompatible Service, Digital has been servicing multivendor environments since 1983. Support has grown to cover more than 1000 products manufactured by more than 200 vendors. This support includes on-site services as well as access to toll-free technical support lines for questions about repair, installation, and operation.

Whatever your service requirements, you may select a single source of quality service for virtually every piece of equipment in your system.

Digital stands behind its PC DECcompatible Service with in-depth product evaluations, proper level of spares, training, support, manpower commitment, and local managers responsible for service planning and delivery.

Digital's Field Service organization is backed by a half-billion-dollar spare parts inventory and supports more than 27,000 service professionals worldwide. Digital's service professionals are trained in total system support PC hardware, software, applications, networks, and non-Digital PCs, and they receive continuous training in the latest service techniques and technologies.

Digital's PC DECcompatible Service provides the end user with a wide range of support services including expert consultation, installation, training, telephone support, and system maintenance—everything needed to increase production quickly:

- Digital offers **priority response** to remedial service requests made during contracted hours of coverage. Hardware remedial support for Digital and non-Digital PCs is available on-site 8:00 A.M. to 5:00 P.M. Optional extended hours of coverage are also available.
- Digital offers **automatic problem escalation** involving all the required technical and management resources if a hardware repair exceeds a predetermined time limit.
- Digital offers **unlimited software telephone support** available around-the-clock, seven-days-a-week, whenever the customer needs assistance. Digital's Customer Support Center is staffed with trained professionals experienced in offering solutions and advice in all aspects of your integration needs.

Digital is one of the largest service and support organizations in the world. The depth and breadth of Digital service means more up time and greater productivity for your networked systems, whether you are responsible for a few PCs in a work group or for hundreds around the world.

▪ Additional Reading and References

The following handbooks and reference materials are detailed sources about Digital's workstations and personal computing products. To obtain a copy of any of these materials, contact your Digital sales representative, or see the following ordering instructions with each item:

Customer Periodicals/Services

- *Product Insight Magazine*

  This magazine contains news from Digital about its latest hardware and software products, applications, and services. It is published 10 times a year. To be added to the mailing list, consult a salesperson, or send name, title, company affiliation, and mailing address to:

  Digital Equipment Corporation
  MKO-1/W83
  Continental Boulevard
  Merrimack, NH 03054-9931.

- Digital's Electronic Store

  The Electronic Store is a free, on-line computer service that helps customers evaluate, select, and purchase products on line. The store is a simple, menu-driven system that requires no expertise or training. Critical ordering information is displayed, such as correct part numbers, accurate pricing, and product availability. Once the order is placed, it is immediately and accurately entered into Digital's order-processing system.

  To register for an account on line, dial 800-332-3366 at 1200/2400 baud from 8 A.M. to midnight EST, with any VT100, VT200, DECmate, PRO, VAXstation, or other PC that emulates a VT100.

- Digital Reference Service

  The Digital Reference Service (DRS) is a Corporate information service that brings to your desktop the most current information about all Digital systems, Digital and third-party software, networking products, customer support services, sales channels, prices, and corporate directions. The full DRS literature set is sent directly to subscribers each quarter and includes six binders for convenient bookshelf access.

  Each quarterly update includes: *Doing Business with Digital, Services, Systems, Applications* (four books summarizing the company, unique to DRS), a complete set of perfect-bound SPDs; the VAX, PDP, Networking, and RealTime Systems and Options Catalogs; The U.S. Price List (for U.S. subscribers); the *Software Handbook* and the *VAX and PDP-11 (third-party) Software Source Books*; *DECdirect PLUS; Educational Services' Digest*; *The Digital Annual Report*; and a subscription to the customer magazine, *Product Insight*. $340 per year (price in the U.S. only and subject to change without notice).

To subscribe, write to:

Digital Equipment Corporation
Reference Service, Dept. 12
CFO1-2/K21
200 Baker Ave.
West Concord, MA 01742

Product Literature

- *VAX Systems and Options Catalog*

The catalog offers descriptive, ordering, and configuring information about Digital's VAX systems, workstations, PCs, terminals and printers, hardware options, software products, and services. This catalog is published quarterly. Ask your Digital sales representative for the most recent copy.

- *Networks and Communications Buyer's Guide*

This guide offers descriptive ordering and configuration information about Digital's networking and communications hardware/software products and networking services. It is published quarterly. Ask your sales representative for the most recent copy.

- *DECdirect PLUS*

To complement your Digital computer system, supporting products such as accessories, supplies, add-on and upgrade products, documentation, and selected hardware options are available for immediate delivery through the *DECdirect PLUS* catalog. Network and personal computing products also are available through *DECdirect PLUS*. Featuring a colorful, informative format, *DECdirect PLUS* makes buying high-quality Digital products easier. For your free copy, call toll-free 800-258-1710, or write to:

Digital Equipment Corporation
Peripherals and Supplies
Group P.O. Box CS2008
Nashua, NH 03061

Information Sheets, Brochures, User Manuals, and Documentation

- Information Sheets/Brochures

  Most of Digital's hardware and software products have individual information sheets or brochures. Ask your sales representative for the availability of the following items:

  – *Simplicity: PCs Integrated with the Enterprise* Network Brochure (EA-31226-58)

  – *Personal Computing Systems Architecture* Brochure (EA-31505-69)

  – *Digital's Network Application Support* (ED-31384-58)

  – *VAX/VMS Services for MS-DOS* Information Sheet (ED-31503-69)

  – *Network Integration for the IBM PC Family* Information Sheet (ED-31504-69)

  – *The DECnet-DOS Family of Software* (EJ-28958-42)

  – *Logicraft's 386Ware and Cardware: MS-DOS Computing Capability for VAX Users* Information Sheet (ED-31531-73)

  – *DECdirect PC Solutions Catalog* (EJ-30856-76)

  – *PC Connectivity Solution Guide* (EJ-31168-58)

  – *Installing Applications with PCSA Software* (EK-VAXIA-IN-002)

  – *WPS-PLUS/DOS* Information Sheet (ED-30670-58)

- Digital Press

  Digital Press, the publishing entity of Digital's Educational Services group, publishes practical, timely books for today's computer community. For further information about Digital Press, write to:

  Digital Press
  Digital Equipment Corporation
  12A Esquire Road
  Billerica, MA 01862-9990

Handbooks and Guidebooks

- *VAX/VMS System Software Handbook*

  This handbook provides information about the VAX/VMS system software. (EB-30905-48)

- *DECconnect Communications System Handbook*

  This handbook describes the individual products, packages, and services that make up the DECconnect Communication System. (EB-28987-42)

- *VAXstation 2000 and MicroVAX 2000 Network Guides*

  These guides include instructions for configuring and installing simple networks using ThinWire Ethernet. Guides are included in the VAXstation 2000 Hardware Information Kit (EK-NETAA-UG-001)

- *VAX Architecture Handbook*

  The handbook gives a description of the system design attributes common to VAX family members. Virtual addressing, data representations, instruction formats, addressing modes, interrupt schemes, and memory management are discussed as well.

- *VAX Hardware Handbook*

  This handbook gives general technical information about the VAX hardware line, including VAX processors, data storage systems and devices, and communication products.

- *A Technical Summary of Digital's VAXstation Family*

  This handbook discusses workstation concepts and designs, including a general overview of workstation features and functions. Digital's worksystems including hardware, operating systems, and systems integration are discussed.

- *VAX/VMS Software Language and Tool Handbook*

  This handbook describes the VAX/VMS operating system, DCL, programming languages, development tools, data communication products, and information management products. (EB-29813-48)

- *Digital's Networks: An Architecture with a Future*

  This book gives a description of the DNA, networking concepts, general configuration guidelines, network functions, and network management. (EB-26013-42)

- *Digital's Solution to Multivendor Networking*

  This book presents an overview of the hardware and software connections that let Digital's systems communicate with those of other manufacturers (primarily IBM systems). (EB-29097-42)

- *VAX Software Source Book*

  This book gives concise descriptions of more than 2500 software products for the VAX family of computers. Products are grouped by industries and generic disciplines and cross-indexed by product name. (ED-31744-46)

- DECconnect *System General Description*

  This description gives the products and services of Digital's DECconnect System. It also reviews the planning and installation processes for building a comprehensive communications network. (EK-DECSY-GD-001)

Glossary

access control list (ACL)
In the VAX/VMS environment, a list that defines users' rights to use a resource or service.

active window
In MS-Windows, the window in which a user is working. Only the active window is affected by commands or other information the user enters.

application disk
A virtual or physical disk that contains MS-DOS application software.

application file service
A file service used to store executable files for MS-DOS applications.

application virtual disk service
A virtual disk used to store executable files for MS-DOS applications.

asynchronous communication
A method of data transmission in which time intervals between transmitted characters can be of unequal length. Transmission is controlled by start and stop elements at the beginning and end of each character.

asynchronous system trap (AST)
(For DECnet) An RSX software interrupt that occurs as a result of an internal significant event such as completion of an I/O request.

AUI
The abbreviation for Attachment Unit Interface. The DEPCA contains an AUI connector, mounted on a separate mounting bezel. The AUI option lets you connect to the Digital standard Ethernet. You can connect to either an Ethernet II transceiver cable or the newer IEEE 802.3 Ethernet transceiver cable.

barrel connector
A female connector for connecting two sections of Ethernet coaxial cable.

baseband
A coaxial cable used for implementing Ethernet. Baseband Ethernet replaces the numerous connecting cables in traditional data networks with a single network cable.

BNC connector
ThinWire network connector, located on the bottom of the DEPCA mounting bracket.

boot
(Short for bootstrap.) In the PCSA environment, to load the MS-DOS operating system into PC workstation memory and start up the PC workstation. See also remote boot.

boot file
A file containing the boot image.

boot image
The minimum set of instructions needed to run a computer, including device drivers, directory structures, and memory management.

cache
A very fast memory that can be used in combination with slower, large-capacity memories.

central processing unit (CPU)
The CPU is the main unit of the computer that contains the circuits controlling interpretation and execution of instructions.

client
A PC workstation connected to a PCSA network, which can access resources on a VAX/VMS server. See also server.

common file service
A file service used to store files to which many users have write access.

control menu
In MS-Windows, the menu listing commands that let users pause, restart, or cancel a print job listed in the spooler queue.

data link
The lowest level of network software, which is the interface between the PC workstation Ethernet controller and higher software levels. The type of data link the PC workstation uses depends on the Ethernet controller the PC workstation has.

data link layer (DLL)
(Ethernet) The highest of the two layers of the Ethernet specification that uses a medium-independent, link-level communication facility on top of the physical channel provided by the physical layers.

DCL
The abbreviation for Digital Command Language. DCL is the standard command interface to Digital's major operating systems.

DDCMP
The abbreviation for Digital Data Communications Message Protocol (DDCMP). DDCMP is a formal set of conventions designed to provide error-free, sequential transmission of data over physical links.

DECnet
Digital networking software that runs on nodes in both LANs and WANs.

DECserver 200
A terminal server that lets users connect multiple terminals and printers to an Ethernet network.

DELNI
The abbreviation for Digital Ethernet Local Network Interconnect. A local network device that provides eight transceiver cable connections. Up to eight devices can connect to the Ethernet network with a DELNI.

DEMPR
The abbreviation for Digital Ethernet Multiport Repeater. A multiport repeater that provides eight ThinWire Ethernet drops (ports for connecting coaxial cable) from a single standard Ethernet connection.

DEPCA
The abbreviation for Digital Ethernet PC Adapter. An Ethernet controller used to connect PCs to the PCSA network as clients.

DEQNA
The abbreviation for Digital Ethernet Q-bus Network Adapter. A high-performance synchronous communications controller for computers based on Q-bus hardware. The DEQNA allows the MicroVAX computer to connect to the Ethernet network.

DESTA
The abbreviation for Digital Ethernet Station Adapter. An Ethernet IEEE 802.3-compliant transceiver that connects intelligent devices that use transceiver cable to the ThinWire Ethernet network.

disk buffer
A block of memory in which the MS-DOS operating system can hold data being read from or written to a disk when the amount of data is not an exact multiple of sector size.

disk server
Software that allows a PC workstation to connect to a VAX/VMS file that acts like a local disk (a "virtual disk") to the PC workstation.

downline load
To transfer data from a host system to a client system over the network.

driver
The software that lets a computer communicate, through the operating system, with a device by controlling all input to, and/or output from, the device.

end node
A network node that cannot forward packets intended for other nodes.

Ethernet backbone
Coaxial cable installed throughout a building to which Ethernet network devices can connect.

Ethernet controller
A device that sends and receives network data on the wires on both server and client. For example, a DEPCA is an Ethernet controller for a PC that is connected to the network.

event
A term specific to DECnet. An event is a network or system-specific occurrence for which the logging component maintains a record. See also event class and event type.

event class
A term specific to DECnet and VAX/VMS. An event class is a particular classification of events. Generally, this follows the DNA architectural layers, with some layers possible containing more that one event class. A class also includes the identification of system-specific events.

event type
A term specific to DECnet and VAX/VMS. A particular type of event, unique within an event class.

external command
The MS-DOS files that are stored as files on a diskette, hard disk, or virtual system disk during installation and read into memory when a user types the command. External commands file names are shown in a directory listing.

faceplate
A wall receptacle that provides the single network connection point for office communication equipment, including data, voice, and video cable devices.

file server
A DECnet network program that allows clients to access existing directories and print queues on a VAX computer.

file service
The availability of directories, subdirectories, and files on a VAX/VMS server. Users can make use of a file service, through a client, with network commands and then store and retrieve data. A file server makes each service accessible to clients.

filter
A command or program that reads input, acts on the input, and then transmits it, usually to a PC workstation or a file.

H4000-BA or Transceiver (T)
A tap on the Ethernet backbone that connects Ethernet devices, such as DELNIs, to the backbone.

internal command
In MS-DOS, the commands stored in the COMMAND.COM file that are read into memory automatically when a PC workstation is booted. Internal commands are not shown in directory listings.

key diskette
A diskette used to start up the PC workstation and make network connections. Files containing PC workstation configuration information, optional user-specific information, and some MS-DOS utilities are stored on the key diskette.

LAD
The abbreviation for Local Area Disk. See virtual disk.

LAN
The abbreviation for Local Area Network. A LAN can span a limited distance, such as a building or cluster of buildings.

LAST
The abbreviation for Local Area System Transport. The network protocol used by the virtual disk server to send and receive data between two computers.

LAT
The abbreviation for Local Area Transport. An Ethernet protocol, used in local area networks, that transfers data on a character-by-character basis. For example, the VT220 terminal emulator uses the LAT protocol to communicate on the Ethernet network.

line echo
A state in which whatever is displayed on the PC workstation screen is simultaneously sent to LPT1 for printing. The screen display is echoed on the printed page.

logical device
A software name that identifies a hardware device to an application or program.

mount
To make a virtual disk available to users on a network.

Network Interconnect (NI)
Digital's name for the Ethernet.

network key disk
A virtual disk that downline loads an operating system to a PC workstation over the network. See also boot file, boot image, remote boot.

node
An individual computer or intelligent device that can communicate with other computers or intelligent devices in a network.

node name
A label that identifies a DECnet node. A DECnet node name has up to six alphanumeric characters, including at least one letter.

packet
A group of bits in a data stream, including data and control elements, that are switched and transmitted together.

parallel
In the context of data transmission, a method of information transfer in which all bits are transmitted simultaneously, rather than sequentially, on different lines or channels. See also serial.

parallel port
The PC workstation hardware component used to connect a parallel, or synchronous, printer to a PC workstation.

parallel printer
A printer that uses synchronous communication.

path name
In MS-DOS, a description of the location of directories and/or files in the operating system. A path name can consist of drives, directories, and files. Each directory and file name is preceded by a backslash.

PC
The abbreviation for Personal Computer.

PCSA
The abbreviation for Personal Computing System Architecture. PCSA is Digital's networking solution for incorporating PCs into the larger VAX-based corporate network.

PC workstation
A PC used to communicate over a network and use the services available on that network. May include the IBM Personal Computer AT, XT, and PC, or IBM-compatible computers.

personal file service
A file service used to store a user's personal files.

personal virtual disk service
A virtual disk used to store a user's personal files. Users have write access to this disk and can store personal files and application data files.

PIF
The abbreviation for Program Information File. In MS-Windows, a file that contains information about how a standard application uses PC workstation resources. MS-Windows uses this information when the user runs the application.

printer driver file
An MS-Windows file to tailor general printing functions for a printer.

printer service
The availability of a printer, connected to a VAX/VMS server. Users can access a printer service, through a client, with network commands and then print files. A file server makes a printer service available to clients.

protocol
A set of rules for formatting and timing the rate of data sent over a network.

redirect
To assign a logical device name to a physical device.

remote boot
A process by which a PC workstation operating system is loaded and started from a network key disk.

RMS
The abbreviation for Record Management Services. The Digital-specific definition defines RMS as a routine that is used to open and close files, read from files, and extend and delete files.

segment
In the context of an Ethernet network, a length of coaxial cable made up of one or more cable sections connected with barrel connectors or T-connectors.

serial
In the context of data transmission, a method of information transfer in which each bit of information is sent sequentially on a single channel.

serial port
The hardware component on a PC workstation used to connect to a serial communication device, such as a modem, terminal, or serial printer. See also serial.

serial printer
A printer that uses asynchronous communication.

server
A VAX/VMS computer or MicroVAX II running PCSA server software that makes the disk, printers, and other devices connected to the computer available as services to clients. See also client.

service
A function available to a client on the network. See also file service, printer service, and virtual disk service.

service name
A label the user or system administrator gives to file, printer, or disk services when making any one of these services available to other users.

session
A logical connection between a PC workstation and a server.

SPD
The abbreviation for Software Product Description. SPDs are Digital-specific. SPDs define the function of a product and minimum hardware needed to support it. They describe software, components, and service.

synchronous communication
A method of data transmission that allows each event to operate in relation to a timing signal. The timing signal synchronizes the transmitter and the receiver, eliminating the need for stop bits and providing efficiency in data transfer.

T-connector
An Ethernet network device that connects ThinWire Ethernet cable to devices in a network.

terminator
A connector used on both ends of an Ethernet network segment. This connector provides the 50-ohm termination resistance needed for the cable.

ThinWire
A Digital Ethernet coaxial cable that is thin and flexible. Thinwire is IEEE 802.3-compliant and used for LANs.

transceiver cable
A cable used to attach a device either to a standard Ethernet segment or to a DESTA connected to a ThinWire Ethernet segment.

UAF
The abbreviation for User Authorization File. A file containing an entry for every user that the system manager authorizes to gain access to the system.

UIC
The abbreviation for User Identification Code. UIC is a pair of numbers assigned to users and to files, global section, common event flag clusters, and mailboxes that specifies the type of access available to the owners, group, world, and system.

virtual
Having the attributes of something, but not actually being it. For example, a virtual disk is space on a VAX/VMS disk accessed through an MS-DOS drive by PC workstation users. The PC workstation user uses the VAX/VMS disk space as if it were an MS-DOS disk.

virtual disk
Same as LAD. Space the disk server program sets aside on a VAX/VMS disk that users can connect to through an MS-DOS drive and on which users can store, create, and maintain MS-DOS files.

virtual disk service
VAX/VMS file created by the disk server program to which PC workstations can connect and use like a local disk. See also LAD.

WPS
Digital's abbreviation for word processing system. It refers to any one of Digital's word processing products such as WPS-PLUS.

Index

E

F

I

J

K

L

M

N

P

R

S

T

V

Integrated Personal Computing Handbook

Reader's Comments

Your comments and suggestions will help us in our continuous effort to improve the quality and usefulness of our handbooks.

What is your general reaction to this handbook? (format, accuracy, completeness, organization, etc.)

_____

_____

_____

What features are most useful? _____

_____

_____

Does the publication satisfy your needs? _____

_____

_____

What errors have you found? _____

_____

_____

_____

Additional comments _____

_____

_____

Name _____

Title _____

Company _____

Address _____

City _____ State _____ Zip _____

EB-32399-69

(staple here)

(please fold here)

No Postage Necessary if Mailed in the United States

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 33 MAYNARD, MASS.

POSTAGE WILL BE PAID BY ADDRESSEE

Digital Equipment Corporation
Corporate Marketing Communications
CFO1-2/M92
200 Baker Avenue
West Concord, MA 01742

digital